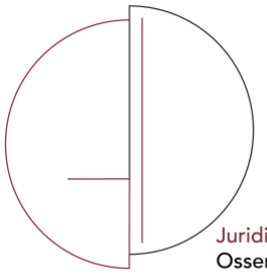

DIRITTO E NUOVE TECNOLOGIE*

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).

* 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. Approvato il 'Digital Services Act': Regolamento (UE) 2022/2065 del 19.10.2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE.

Il 27 ottobre 2022 è stato pubblicato nella Gazzetta ufficiale dell'Unione Europea il Regolamento (UE) 2022/2065 "relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)", noto come *Digital Services Act* (DSA) (di seguito anche solo il "**Regolamento**"). Il Regolamento rappresenta l'ultima tappa di un percorso avviato nel dicembre 2020 dalla Commissione europea con la proposta da COM(2020) 825 final (su cui v. la notizia sub 3 nel numero 1/2021 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio.pdf).

L'approvazione del testo finale del Regolamento è arrivata dopo un susseguirsi di emendamenti, prima accolti e poi rigettati, per tornare in parte alla proposta originaria. In particolare, il 20 gennaio 2022 sono stati proposti degli emendamenti dal Parlamento Europeo, ai quali sono seguiti dei negoziati tra Consiglio UE, Commissione europea e Parlamento Europeo, con l'esito di un accordo politico nel successivo mese di aprile. Nel giugno 2022, però, la maggioranza degli eurodeputati si è opposta al testo inviato dalla Presidenza francese del Consiglio dell'UE, in quanto non ritenuto conforme all'accordo politico raggiunto poco prima. Il testo del Regolamento è stato poi approvato all'unanimità dal Parlamento Europeo il 5 luglio 2022, per arrivare, successivamente, e con qualche modifica, al testo pubblicato il 27 ottobre. Il Regolamento è destinato a trovare applicazione quasi integrale dal 17 febbraio 2024, salvo alcuni aspetti che hanno un'applicazione anticipata dallo scorso 16 novembre e che riguardano le piattaforme dei *big player* e l'attività della Commissione europea. Segnatamente, le piattaforme *online* avranno 3 mesi di tempo fino al 17 febbraio 2023 per comunicare il numero di utenti finali attivi sui loro siti *web*. Sulla base di questi dati, la Commissione valuterà se una piattaforma debba essere designata come piattaforma *online* o motore di ricerca di grandi dimensioni. Tale designazione da parte della Commissione comporterà l'obbligo, entro 4 mesi, di adeguarsi alle previsioni del Regolamento, compreso lo svolgimento e la presentazione alla Commissione del primo esercizio annuale di valutazione del rischio.

Come nella proposta di regolamento, si delinea una logica proporzionale e cumulativa nell'imposizione di obblighi, che aumentano e si sommano a mano a mano che i fornitori di servizi di intermediazione siano qualificabili come *hosting*, piattaforme *online* o *very large online platforms*, con l'aggiunta, però, di un ulteriore specifico riferimento ai motori di ricerca *online*, al destinatario attivo di una piattaforma *online* e al destinatario attivo di un motore di ricerca *online*.

Alcuni chiarimenti si notano sin dalla formulazione dell'art. 1, che consta di un nuovo paragrafo, ove si specifica che il Regolamento mira a contribuire al funzionamento del mercato interno dei servizi intermediari, stabilendo norme armonizzate per un ambiente online sicuro, prevedibile, affidabile e che faciliti l'innovazione, tutelando in modo effettivo i diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione Europea e garantendo effettività anche nella protezione dei consumatori. Con riferimento all'ambito di applicazione del Regolamento, una diversa formulazione rispetto a COM(2020) 825 si rinviene anche nel Considerando 9), ove si esplicita che il Regolamento dovrebbe integrare, ma non pregiudicare, l'applicazione delle norme derivanti da altri atti del diritto dell'Unione e che gli Stati membri non dovrebbero adottare o mantenere prescrizioni nazionali aggiuntive in relazione alle questioni che rientrano nell'ambito di applicazione del Regolamento. Fermo restando che ciò non preclude la possibilità di applicare altre normative nazionali ai prestatori di servizi intermediari, qualora le stesse perseguano legittimi obiettivi di interesse pubblico diversi da quelli del Regolamento.

Interessanti sono anche alcune precisazioni che si riferiscono ai contenuti e alle attività illegali. Il Considerando 12) del Regolamento chiarisce che il concetto di contenuto illegale dovrebbe rispecchiare ampiamente le norme vigenti nell'ambiente *offline*. Il Considerando 20) specifica che il solo fatto che un servizio offra trasmissioni cifrate o qualsiasi altro sistema che renda impossibile l'identificazione dell'utente non dovrebbe di per sé essere considerato come un'agevolazione di attività illegali.

Rispetto alla proposta di regolamento di dicembre 2020, sono interessanti alcuni chiarimenti su cosa debba intendersi per conoscenza o consapevolezza effettiva di contenuti e attività

illegali. Il Considerando 22) del Regolamento esplicita che tale conoscenza o consapevolezza effettiva non può essere considerata acquisita per il solo motivo che il prestatore sia consapevole, in senso generale, del fatto che il suo servizio è utilizzato anche per memorizzare contenuti illegali. Inoltre, la circostanza che il prestatore proceda a un'indicizzazione automatizzata delle informazioni, oppure utilizzi una funzione di ricerca basata sul profilo o sulle preferenze dei destinatari del servizio, non è un motivo sufficiente per considerare che il prestatore abbia una conoscenza «specifica» di attività illegali realizzate sulla medesima piattaforma o di contenuti illegali ivi memorizzati.

La particolare attenzione del Regolamento alla tutela del consumatore è confermata dalla introduzione della sezione quarta, che prevede disposizioni aggiuntive applicabili ai fornitori di piattaforme *online* che consentono ai consumatori di concludere contratti a distanza con gli operatori commerciali. Ivi si impongono precisi obblighi ai fini di consentire ai consumatori la tracciabilità degli operatori commerciali. In particolare, se l'art. 30 del Regolamento ripropone in gran parte i contenuti dell'art. 22 di COM(2020) 825 final, l'art. 31 introduce disposizioni dettagliate circa la conformità nella progettazione delle interfacce *online* per i fornitori di piattaforme che consentono ai consumatori di concludere contratti a distanza. Si prevede, in particolare, che le piattaforme debbano essere progettate e organizzate in modo da consentire agli operatori commerciali di fornire ai consumatori almeno le informazioni necessarie per l'identificazione chiara e inequivocabile dei prodotti o dei servizi promossi o offerti, oltre a qualsiasi indicazione che identifichi il commerciante, come il marchio, il simbolo o il logo e, se del caso, le informazioni relative all'etichettatura e alla marcatura, conformemente alle norme del diritto dell'Unione applicabile in materia di sicurezza e conformità dei prodotti. Anche l'art. 32 del Regolamento presenta ulteriori novità per il consumatore nel caso di acquisto di prodotti o servizi illegali da un operatore commerciale che abbia svolto la sua attività per il tramite della piattaforma *online*. In particolare, il fornitore della piattaforma deve verificare se ha i recapiti del consumatore e informarlo direttamente, oppure laddove non disponga dei recapiti di tutti i consumatori interessati, deve rendere disponibili al pubblico, e facilmente accessibili sulla propria interfaccia *online*, le informazioni concernenti il prodotto o servizio illegale, l'identità dell'operatore commerciale ed eventuali mezzi di ricorso pertinenti.

A differenza di COM(2020) 825 final, nell'attuale formulazione del Considerando 13) del Regolamento si rinviene esplicita attenzione ai servizi di *cloud computing* e di *web hosting*. Detto Considerando, pur essendo meno dettagliato nella versione di ottobre rispetto a quella di luglio, espressamente prevede che tali servizi non dovrebbero essere considerati una piattaforma *online* ove la diffusione di contenuti specifici al pubblico costituisca una caratteristica minore e accessoria o una funzionalità minore di tali servizi. Lo stesso Considerando specifica che i servizi di *cloud computing* o di *web hosting* quando fungono da infrastruttura non dovrebbero essere considerati di per sé una diffusione al pubblico di informazioni.

Ulteriori interessanti specificazioni, rispetto a COM(2020) 825, riguardano proprio il concetto di "diffusione al pubblico" che nel testo definitivo del Regolamento prevede che qualora l'accesso alle informazioni richieda la registrazione o l'ammissione a un gruppo di destinatari del servizio, tali informazioni dovrebbero essere considerate diffuse al pubblico solo se i destinatari del servizio che intendono accedervi siano automaticamente registrati o ammessi senza una decisione o una selezione umana che stabilisca a chi concedere l'accesso. Il riferimento sul punto è alla nuova formulazione del Considerando 14) del Regolamento.

Un' ulteriore specificazione riguarda le attività volontarie poste in essere dai prestatori di servizi intermediari per individuare, identificare e contrastare i contenuti illegali. Si tratta di attività disciplinate dall'art. 7 del Regolamento, corrispondente all'art. 6 di COM(2020) 825 final. In particolare, il richiamato articolo 7 ribadisce che il solo fatto che i prestatori di servizi intermediari intraprendano tali attività non fa venir meno l'esenzione di responsabilità prevista dal Regolamento, ma aggiunge che ciò può verificarsi soltanto se tali attività sono svolte in buona fede e in modo diligente. Sul punto, di rilievo è anche la nuova formulazione del Considerando 26) del Regolamento, nella parte in cui chiarisce che l'agire in buona fede e in modo diligente dovrebbe includere l'agire in modo obiettivo, non discriminatorio e proporzionato, tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte e fornendo le necessarie garanzie contro la rimozione ingiustificata di contenuti legali. Nel Considerando 41) del Regolamento si ritorna sul punto chiarendo che gli obblighi armonizzati in materia di dovere di

diligenza, che dovrebbero essere ragionevoli e non arbitrari, sono necessari per affrontare obiettivi di interesse pubblico come la tutela degli interessi legittimi dei destinatari del servizio, il contrasto delle pratiche illegali e la tutela dei diritti fondamentali. Si aggiunge, in modo quanto meno discutibile, che gli obblighi in materia di dovere di diligenza sono indipendenti dalla questione della responsabilità dei prestatori di servizi intermediari che deve, pertanto, essere valutata separatamente.

Ulteriori novità riguardano il contenuto del Considerando 39) del Regolamento nella parte relativa agli obblighi di fornire informazioni sui meccanismi di ricorso a disposizione del prestatore di servizi intermediari e del destinatario del servizio che ha fornito i contenuti. Si prevede la possibilità che i coordinatori dei servizi sviluppino strumenti e orientamenti nazionali al fine di facilitare l'accesso a tali meccanismi da parte dei destinatari del servizio e che le competenti autorità giudiziarie o amministrative nazionali possano emettere, sulla base del diritto dell'Unione o nazionale applicabile, un ordine di ripristino dei contenuti, qualora tali contenuti fossero conformi alle condizioni generali del prestatore di servizi intermediari, ma siano stati erroneamente considerati illegali da tale prestatore e siano stati rimossi.

La necessità di rispettare i diritti fondamentali di tutte le persone interessante nel delicato problema del rimuovere o disabilitare l'accesso ai contenuto illegali, senza pregiudicare indebitamente la libertà di espressione e di informazione dei destinatari dei servizi, è ribadita dai Considerando 51) e 52) che, a tal fine, fanno riferimento alla necessità di una notifica di segnalazione mirata e ad un agire senza indugio qualora siano notificati presunti contenuti illegali che comportano una minaccia per la vita o la sicurezza delle persone, in particolare tenendo conto del tipo di contenuto illegale. Il dato è ripetuto più volte anche con l'introduzione, nel Regolamento, di nuovi Considerando, come per esempio il 53), che insiste soprattutto sulla necessità di una spiegazione dettagliata dei motivi sia della segnalazione sia dell'eventuale disabilitazione o rimozione dei contenuti. Maggiori cautele riguardano l'identità della persona o dell'entità che ha presentato la segnalazione, in particolare laddove si indica che si dovrebbe rivelarla solo se tale informazione è necessaria per identificare l'illegalità del contenuto. Il dato si evince dalla nuova formulazione del Considerando 54) del Regolamento.

Rispetto a COM(2020) 825, nuove sono anche le previsioni in tema di divieto all'uso di c.d. "*dark pattern*", ossia dei "*percorsi oscuri*" sulle interfacce delle piattaforme *online* che distorcono o compromettono in misura rilevante, intenzionalmente o di fatto, la capacità dei destinatari del servizio di compiere scelte o decisioni autonome e informate. Si tratta per esempio, come specifica il Considerando 67) del Regolamento, di scelte di progettazione volte a indirizzare il destinatario verso azioni che apportano benefici al fornitore di piattaforme *online*, ma che possono non essere nell'interesse dei destinatari, presentando le scelte in maniera non neutrale. Si pensi all'attribuzione di maggiore rilevanza a talune componenti visive, auditive o di altro tipo, nel chiedere al destinatario del servizio di prendere una decisione oppure alla prassi di rendere la procedura di cancellazione di un servizio notevolmente più complessa di quella di aderirvi, o rendendo talune scelte più difficili o dispendiose in termini di tempo rispetto ad altre.

Il dato è ribadito nella formulazione del nuovo articolo 25 del Regolamento, ai sensi del quale 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.

Da segnalare in questo contesto è inoltre la previsione dell'art. 26, par. 3 del Regolamento, laddove si prevede che i fornitori di piattaforme *online* non possono presentare pubblicità ai destinatari del servizio basate sulla profilazione (come definita all'articolo 4, punto 4), del regolamento (UE) 2016/679: GDPR) utilizzando le categorie speciali di dati personali di cui all'articolo 9, par. 1, del GDPR.

Anche sulla trasparenza dei sistemi di raccomandazione ci sono delle precisazioni che emergono dalla diversa formulazione dell'art 27 del Regolamento rispetto alla previsione del corrispondente articolo art. 29 COM(2020) 825. Nello specifico, il riferimento è al paragrafo 2 dell'art. 27 del Regolamento, ove si dispone che i principali parametri che chiariscono il motivo per cui talune informazioni sono suggerite al destinatario del servizio devono comprendere alcuni elementi e, segnatamente i criteri più significativi per determinare le informazioni suggerite al destinatario del servizio e le ragioni per l'importanza relativa di tali parametri.

Ulteriore novità importante, che merita di essere segnalata, è la maggiore attenzione alla protezione *online* dei minori, alla quale è dedicato l'art. 28 del Regolamento. Si richiede, infatti, che i fornitori di piattaforme *online* accessibili ai minori adottino misure adeguate e proporzionate per garantire un

elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori. Sono previsti specifici divieti anche con riferimento alla pubblicità basata sulla profilazione, qualora i fornitori di piattaforme siano consapevoli, con ragionevole certezza, che il destinatario del servizio sia un minore.

Nella stessa direzione muove la nuova formulazione dell'art. 14 del Regolamento che prevede, al par. 3, che se un servizio intermediario è principalmente destinato a minori o è utilizzato in prevalenza da questi, il prestatore di tale servizio deve spiegare, in modo comprensibile per i minori, le condizioni e le restrizioni che si applicano all'utilizzo del servizio.

La protezione dei minori, come importante obiettivo politico dell'Unione, è reso esplicito dal Considerando 71) del Regolamento. Non vi erano previsioni uguali in COM(2020) 825, nonostante nei Considerando non mancassero generici riferimenti alla necessità di tutela di minori e soggetti vulnerabili.

Restano due aspetti che meritano di essere segnalati come novità del Regolamento (UE) 2022/2065 rispetto alla proposta di COM(2020) 825 final. Il primo riguarda la valutazione del rischio di cui all'art. 34, che corrisponde all'art 26 di COM(2020) 825 final, dal quale si differenzia nel par.1, per i riferimenti alla diligenza nella valutazione dei rischi sistemici, alla possibilità che tali rischi possano derivare da sistemi algoritmici, alla previsione che la valutazione del rischio debba essere specifica per i loro servizi e proporzionata ai rischi sistemici, tenendo in considerazione la loro gravità e la loro probabilità.

Anche nel riferimento ai rischi sistemici, il par. 1 dell'art. 34 del Regolamento presenta delle modifiche rispetto a quanto previsto da COM(2020) 825 final, in particolare perché si tiene conto di eventuali effetti negativi, anche solo prevedibili, per l'esercizio dei diritti fondamentali. Vi è, al riguardo, un espresso riferimento alla dignità umana, alla tutela dei dati personali e alla libertà e al pluralismo dei media, oltre all'aggiunta del riferimento esplicito a qualsiasi effetto negativo, attuale o prevedibile, in relazione alla violenza di genere, alla protezione della salute pubblica e dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona.

Significativo appare, inoltre, il riconoscimento in favore dei destinatari del servizio, ai sensi dell'art. 54 del Regolamento, di un diritto al risarcimento in presenza di danni o perdite subite a causa di una violazione degli obblighi stabiliti dal Regolamento stesso da parte dei fornitori di servizi intermediari.

Non mancano differenze e modifiche con riferimento alle previsioni relative alla risoluzione extragiudiziale delle controversie, all'apparato burocratico disegnato per controllare il rispetto del Regolamento ed anche all'articolazione delle sezioni del Regolamento stesso, con delle differenze non sempre solo formali. Per esempio, la previsione dell'obbligo di attivarsi senza alcun *input*, nel caso di conoscenza di informazioni che fanno sospettare che sia stato commesso, si stia commettendo o probabilmente sarà commesso un reato grave che comporta una minaccia per la vita o la sicurezza delle persone, era disciplinato dall'art. 21 di COM(2020) 825 final, che corrisponde all'attuale articolo 18 del Regolamento. La modifica non è solo numerica, in quanto si tratta di un obbligo che non riguarda più le disposizioni aggiuntive applicabili ai fornitori di piattaforme *online*, ma per effetto dello spostamento della previsione dalla sezione 3 alla sezione 2 del Regolamento, riguarda anche i prestatori di servizi di memorizzazione di informazioni.

SARA TOMMASI

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R2065&from=EN

2. Approvato il 'Digital Markets Act': Regolamento (UE) 2022/1925 del 14.09.2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive 2019/1937/UE e 2020/1828/UE.

Il 14 settembre 2022, dopo meno di due anni dalla proposta della Commissione europea COM(2020) 842 final del 15 dicembre 2020 (di seguito la "**Proposta**": su cui v. la notizia n. 4 nel numero 1/2021 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio.pdf), è intervenuta l'approvazione del Regolamento 2022/1925/UE del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive 2019/1937/UE e 2020/1828/UE (c.d. *Digital Markets Act* o regolamento sui mercati digitali, di seguito "**DMA**" o il "**Regolamento**").

Perno della strategia digitale dell'Unione Europea (*Shaping Europe's Digital Future*:

https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf), il DMA appronta una disciplina dei mercati digitali ponendo enfasi sui servizi di piattaforma di base forniti dai cc.dd. *gatekeepers* (controllori dell'accesso).

Il dato empirico mostra che le caratteristiche di questi servizi digitali, ossia gli effetti di rete, le estreme economie di scala e l'estrazione di dati personali su larga scala, sono foriere di pericolose concentrazioni di potere economico nelle mani di un numero ridotto di imprese di grandi dimensioni, che esercitano un significativo grado di dipendenza sia degli utenti commerciali sia degli utenti finali (cfr. *Considerando* 2) DMA). Ne derivano, come corollari, l'esistenza di barriere elevate all'ingresso e all'uscita e una ridotta contendibilità dei mercati di riferimento (cfr. *Considerando* 3) DMA). Su questo retroterra si appunta il rischio di gravi squilibri di potere contrattuale, che si sostanziano in pratiche sleali e nell'imposizione di condizioni inique, tanto per gli utenti commerciali quanto per gli utenti finali. Inoltre, si teme che i *gatekeeper* tengano condotte tali da non consentire la piena comprensione dei vantaggi che essi ritraggono dagli apporti dell'utenza (cfr. *Considerando* 33) DMA).

L'ambito applicativo del Regolamento è, dunque, tangente alla materia della concorrenza *tout court* (il cui regime – artt. 101 e 102 TFUE *in apicibus* – resta impregiudicato *ex* art. 1, par. 6 DMA), e ad essa si accosta, in chiave integrativa, attraverso un quadro uniformato di tutela dell'interesse giuridico a che i mercati in cui sono presenti *gatekeeper* siano e rimangano equi e contendibili (v. art. 1, parr. 1 e 2 DMA).

Preme evidenziare un dato cruciale, che emerge già nella parte iniziale del Preambolo del Regolamento: il regime in analisi poggia sulla correlazione tra due nozioni fondamentali, cioè a dire quelle di *gatekeeper* e di servizio di piattaforma di base. Come chiarito al Considerando 15), infatti, il fatto che un servizio digitale costituisca un servizio di piattaforma di base non solleva di per sé preoccupazioni sufficientemente gravi in termini di contendibilità o pratiche sleali; esse emergono solo nei casi in cui tale servizio costituisce un punto di accesso importante ed è gestito da un'impresa che può vantare un impatto significativo nel mercato interno e una posizione consolidata e duratura o da un'impresa che prevedibilmente vanterà una simile posizione nel prossimo futuro.

Il primo concetto chiave è quello di "servizi di piattaforma di base". Sul punto, all'art. 2, lett. *g*) e *h*) DMA è dato riscontrare, rispetto alla Proposta, un ampliamento del perimetro definitorio che, attualmente, ricomprende i servizi di *browser web* e gli assistenti virtuali.

Rispetto alla Proposta, rimane inalterata la nozione di *gatekeeper*, di cui all'art. 3 DMA, che compete a quelle imprese che: *i*) hanno un impatto significativo sul mercato interno; *ii*) gestiscono un servizio di piattaforma di base che costituisce un punto di accesso (*gateway*) tra gli utenti commerciali e gli utenti finali, e (*iii*) detengono una posizione consolidata e duratura nel proprio settore di mercato (o si prevede che la acquisiranno in futuro). La competenza ad attribuire la qualifica si conferma della Commissione e si correda, al par. 3, dei pertinenti obblighi di comunicazione e, all'art. 4 DMA, del potere di riesame dello *status*. Variazioni, eminentemente quantitative, interessano la presunzione relativa di cui al par. 2, lett. *a*) nel senso di un innalzamento delle soglie dimensionali. Il primo requisito si ritiene soddisfatto se l'impresa raggiunge un fatturato annuo nell'Unione pari o superiore a 7,5 miliardi di euro in ciascuno degli ultimi tre esercizi finanziari o se la sua capitalizzazione di mercato media o il suo valore equo di mercato equivalente era quanto meno pari a 75 miliardi di euro nell'ultimo esercizio finanziario, e se essa fornisce lo stesso servizio di piattaforma di base in almeno tre Stati membri. Il secondo può presumersi in caso di prestazione di un servizio di piattaforma di base che, nell'ultimo esercizio finanziario, annovera almeno 45 milioni di utenti finali attivi su base mensile, stabiliti o situati nell'Unione, e almeno 10.000 utenti commerciali attivi su base annua stabiliti nell'Unione, identificati e calcolati conformemente alla metodologia e agli indicatori di cui all'allegato al DMA (c'è un solo allegato). Infine, il terzo requisito può presumersi se le soglie di cui alla lettera *b*) sono state raggiunte in ciascuno degli ultimi tre esercizi finanziari.

Giova precisare che, trattandosi di presunzione *iuris tantum*, l'operatore economico è ammesso a fornire la prova contraria ai sensi del par. 5.

Ciò posto, è opportuno porre l'accento su un aspetto fortemente indicativo della linea di politica del diritto seguita dal DMA. Il legislatore europeo si è premurato in più punti di prevedere salvaguardie avverso la possibile obsolescenza delle prescrizioni a causa del mutamento tecnologico e delle dinamiche di mercato. Sebbene si tratti di un regolamento, e debba parlarsi perciò di uniformazione, con relativa assunzione del monopolio disciplinare in materia, il quadro si pone come *level playing field* e, dunque, come statuto di base suscettibile di (auto)integrazione. In quest'ottica, entrambe le fondamentali nozioni di *gatekeeper* e di servizi di piattaforma di base possono essere ampliate dalla Commissione ai

sensi, rispettivamente, degli artt. 17 e 19 DMA, previo esperimento di una pertinente indagine di mercato (art. 16 DMA).

Cuore pulsante del regolamento è l'insieme dei divieti e degli obblighi prescritti ai *gatekeeper* al Capo III e distribuiti lungo gli artt. 5, 6 e 7 DMA. Tra i principali, possono annoverarsi i divieti posti al *gatekeeper* dall'art. 5, par. 2 DMA di: *a*) trattamento, ai fini della fornitura di servizi pubblicitari *online*, dei dati personali degli utenti finali che utilizzano servizi di terzi che si avvalgono di servizi di piattaforma di base; *b*) combinare i dati personali provenienti dal pertinente servizio di piattaforma di base con dati personali provenienti da altri servizi di piattaforma di base o da eventuali ulteriori servizi forniti dal *gatekeeper* o con dati personali provenienti da servizi di terzi; *c*) utilizzare in modo incrociato dati personali provenienti dal pertinente servizio di piattaforma di base in altri servizi forniti separatamente dal *gatekeeper*, compresi altri servizi di piattaforma di base, e viceversa; *d*) far accedere con registrazione gli utenti finali ad altri servizi del *gatekeeper* al fine di combinare dati personali. Tuttavia, si tratta in tutti questi casi di divieti che non operano laddove il *gatekeeper* abbia ottenuto un consenso dagli interessati ai sensi degli artt. 4, n.11 e 7 del Regolamento (UE) 2016/679 (GDPR). A tal fine, sempre nell'art. 5, par. 2 DMA è previsto che se l'utente finale ha negato o revocato il consenso, il *gatekeeper* non possa ripetere la sua richiesta di consenso per la stessa finalità più di una volta nell'arco di un anno. In ogni caso, tuttavia, l'ultima proposizione dell'art. 5, par. 2 DMA, prevede che non è pregiudicata per il *gatekeeper* la facoltà di avvalersi delle basi del trattamento dei dati personali di cui all'art. 6, par. 1 lettere *c)* (obbligo legale al quale è soggetto il titolare del trattamento), *d)* (salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica) ed *e)* (esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento) del GDPR.

Ai sensi dell'art. 9 DMA, l'operatività di una o più prescrizioni è suscettibile di sospensione, con decisione motivata della Commissione, ove un'impresa dimostri che l'osservanza metterebbe a rischio, a causa di circostanze eccezionali ed eccedenti la propria sfera di controllo, la redditività economica della sua attività nell'Unione. Questa possibilità deve ritenersi esplicazione del principio di proporzionalità delle misure in funzione degli obiettivi perseguiti, che percorre trasversalmente il regolamento (*inter alia,* cfr. Considerando 28) e 66) DMA).

L'applicazione di uno o più obblighi specifici può financo escludersi laddove, per motivi di salute pubblica e sicurezza pubblica (secondo l'interpretazione della CGUE; cfr. Considerando 67) DMA) la Commissione, *ex officio* ovvero su impulso di parte, ritenga di emanare una decisione di esclusione ai sensi dell'art. 10 DMA.

Come sopra accennato, alla rapida evoluzione tecnologica e dei mercati il legislatore europeo risponde, oltre che – s'intende – con l'echeggiata premura per la proporzionalità delle misure, soprattutto con una regolazione programmaticamente flessibile. In quest'ottica, ai sensi dell'art. 12 DMA, la Commissione, mediante l'agile strumento della legislazione delegata, può aggiornare gli obblighi di cui agli artt. 5 e 6 DMA, con i limiti di cui al par. 2 dell'art. 12 DMA. Come evidenziato al Considerando 69 DMA, le integrazioni sono da adottare esclusivamente a valle di indagini approfondite e capillari sulla natura e sull'impatto di pratiche specifiche sul mercato, per sondare adeguatamente la slealtà e la portata limitativa della contendibilità.

Particolare enfasi è posta al contrasto all'elusione della disciplina e, in particolare, delle soglie quantitative di cui all'art. 3, par. 2 DMA. In proposito, l'art. 13 DMA pone un secco divieto di segmentare, dividere, suddividere, frammentare o separare i servizi mediante mezzi contrattuali, commerciali, tecnici o di qualsiasi altro tipo, e precisa che nessuna di tali pratiche impedisce alla Commissione di designare l'impresa come *gatekeeper*, ordinando, se del caso, la trasmissione di tutte le informazioni necessarie.

Completano il Capo III l'obbligo di informare la Commissione sui progetti di concentrazione ai sensi dell'art. 3 Reg. 2004/129/UE (art. 14 DMA) e l'obbligo di audit (art. 15 DMA).

In caso di inosservanza degli obblighi di cui agli artt. 5, 6, o 7 DMA, è previsto che la Commissione adotti, sulla base delle risultanze dei controlli informativi e/o ispettivi, una decisione di esecuzione (art. 29 DMA) in cui si dia conto: delle singole violazioni; delle misure di cui all'art. 8, par. 2 DMA; delle misure provvisorie adottate *ex* art. 24 DMA; degli impegni giuridicamente vincolanti assunti dal *gatekeeper* ai sensi dell'art. 25 DMA; dei rimedi in caso di inosservanza sistemica *ex* art. 18, par. 1 DMA. Nel provvedimento, la Commissione può inoltre irrogare ammende il cui importo non supera il 10% del fatturato totale realizzato a livello mondiale nel corso del precedente esercizio finanziario (art. 30, par. 1 DMA) ovvero fino al 20% del fatturato totale realizzato a livello mondiale nel corso del

precedente esercizio finanziario, se constata che il *gatekeeper* ha commesso, in relazione allo stesso servizio di piattaforma di base, un'infrazione identica o simile a una già rilevata con decisione negli otto anni precedenti (art. 30, par. 2 DMA).

Alle sanzioni pecuniarie si accompagna, nei casi di inosservanza sistematica, il potere di adozione, da parte della Commissione, di atti di esecuzione che impongono all'impresa l'assunzione di qualsiasi rimedio comportamentale o strutturale proporzionato e necessario per garantire l'effettivo rispetto del regolamento (art. 18, par. 1 DMA). L'inosservanza si qualifica come sistematica laddove la Commissione abbia adottato negli ultimi otto anni almeno tre decisioni di esecuzione a norma dell'art. 29 DMA in relazione a uno dei suoi servizi di piattaforma di base.

VALENTINO RAVAGNANI

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R1925&from=EN

3. Approvato il 'DORA': Regolamento (UE) 2022/2554 del 14.12.2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011

Nella Gazzetta ufficiale dell'Unione europea del 27.12.2022 è stato pubblicato il Regolamento (UE) 2022/2554 del 14.12.2022 relativo alla resilienza operativa digitale per il settore finanziario (di seguito solo il "**Regolamento**" o "**DORA**", acronimo per *Digital Operational Resilience Act*). Si tratta del testo rispondente al documento P9_TA(2022)0381 del 10 novembre 2022 con il quale il Parlamento europeo approvava, con alcune modifiche frutto di un compromesso col Consiglio, la proposta di regolamento COM(2020)0595.

Il Regolamento si inserisce nel "Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo" elaborato nel 2018 dalla Commissione europea. Il testo finale del DORA si pone in continuità anche col parere congiunto emesso nell'aprile 2019 da EBA, ESMA ed EIOPA (di seguito le Autorità Europee di Vigilanza o "**AEV**") che invocava "*l'adozione di un approccio coerente ai rischi informatici nel settore finanziario e si raccomandava di potenziare, in maniera proporzionata, la resilienza operativa digitale*".

Il settore della finanza è stato fortemente interessato dall'evoluzione dell'*Information and Comunication Technology* (c.d. "**ICT**" o "**TIC**" nell'acronimo italiano) tanto che quest'ultima ha *"conquistato un ruolo essenziale nella fornitura di servizi finanziari*" (Considerando 2) DORA). Soprattutto alla luce di possibili attacchi informatici, è riconosciuto che tale "interconnessione" tra finanza e ICT può rappresentare una criticità del sistema finanziario, particolarmente per quegli enti con un ruolo "sistemico" nel mercato a causa delle loro dimensioni (cfr. Considerando 3) DORA e il riferimento ivi contenuto al Comitato europeo per il rischio sistemico – CERS/ESRB dal suo acronimo in lingua inglese: *European Systemic Risk Board*).

All'evoluzione tecnologica, inoltre, non si è affiancata un'evoluzione normativa che, finora, si mostra frammentata e, sostanzialmente, di livello nazionale. Ecco, dunque, che il Regolamento "*mira a consolidare e aggiornare i requisiti in materia di rischi informatici nell'ambito dei requisiti in materia di rischi operativi che sono stati finora trattati separatamente in vari atti giuridici dell'Unione*" e "*colma pertanto le lacune o pone rimedio alle incoerenze di taluni fra i precedenti atti legislativi* … [nds, Esso] *dovrebbe altresì accrescere la consapevolezza dei rischi informatici e riconoscere che gli incidenti connessi alle TIC e la mancanza di resilienza operativa potrebbero compromettere la solidità delle entità finanziarie*" (Considerando 12) DORA). Il Regolamento si inserisce in un percorso normativo dell'UE dove si colloca anche il Regolamento (UE) 2022/858 relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito (c.d. **Regolamento DLT**) (su cui v. notizia n. 2 nel numero 2/2022 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2022/08/Osservatorio-2-2022.pdf) e la proposta di **Regolamento sui mercati delle criptovalute** (c.d. MiCAR, acronimo per *Markets in Crypto-Assets Regulation*), (su cui v. notizia n. 3 nel numero 2/2022 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2022/08/Osservatorio-2-2022.pdf).

I destinatari del DORA, chiamati "entità finanziarie" (art. 2.2 DORA), sono sia soggetti tradizionali (ad esempio, banche e assicurazioni), sia "*fornitori di servizi per le cripto-attività*", sia i "*fornitori terzi di servizi TIC*" (art. 2.1 DORA).

L'art. 3 del Regolamento elenca una serie di definizioni, mentre il successivo art. 4 richiama il principio di proporzionalità, sancito anche nel considerando 13, per cui le norme del DORA dovranno essere applicate *"tenendo conto delle …*

dimensioni e del … profilo di rischio complessivo, nonché della natura, della portata e della complessità dei loro servizi, delle loro attività e della loro operatività".

L'art. 1 descrive l'oggetto del Regolamento che sostanzialmente può dividersi in 5 pilastri, similmente a quanto ipotizzato nella precedente versione del testo, come qui di seguito riassunti.

I. Governance e organizzazione (art. 5 DORA)

Le entità finanziarie devono predisporre "*un quadro di gestione e di controllo interno che garantisca una gestione efficace e prudente di tutti i rischi informatici, … al fine di acquisire un elevato livello di resilienza operativa digitale*" (art. 5). L'organo amministrativo ha "*la responsabilità generale di definire e approvare la strategia di resilienza operativa digitale*" e a tal fine deve: i) predisporre "*politiche miranti a garantire il mantenimento di standard elevati di disponibilità, autenticità, integrità e riservatezza dei dati*"; ii) definire "*chiaramente ruoli e responsabilità per tutte le funzioni connesse alle TIC"* e iii) stabilire *"adeguati meccanismi di governance al fine di garantire una comunicazione, una cooperazione e un coordinamento efficaci e tempestivi*" tra le menzionate funzioni (art. 5). All'organo gestionale compete anche l'approvazione, supervisione e riesame dei piani di risposta e ripristino delle infrastrutture ICT in seguito a attacchi informatici.

Vale la pena precisare che le suddette disposizioni sono coerenti con le Linee guida dell'EBA (EBA/GL/2019/04) sulla sicurezza e gestione del rischio ICT e dell'EIOPA (EIOPA-BoS-20/600) sulla sicurezza e governance ICT.

II. Risk management (artt. 6 – 16 DORA)

L'art. 6 si preoccupa di stabilire che le entità finanziarie istituiscano un quadro per la gestione dei rischi informatici "*solido, esaustivo e adeguatamente documentato*" che comprenda "*almeno*" strategie e procedure per proteggere i dati e per assicurare la resilienza e continuità delle attività ICT (art. 11).

Con la sola eccezione delle microimprese, per cui il Regolamento non stabilisce una tempistica, il quadro per la gestione dei rischi informatici deve essere riesaminato annualmente e, comunque, in occasione di gravi incidenti informatici o su richiesta delle AEV, che possono sempre chiedere informazioni sul quadro generale.

Le entità finanziarie devono costantemente monitorare e aggiornare le proprie strategie di resilienza e infrastrutture digitali, che devono essere proporzionate alle proprie dimensioni, affidabili e resilienti (art. 7 e 9). Come anticipato, alle entità finanziarie spetta anche l'individuazione delle funzioni aziendali che utilizzano strumenti ICT (art. 8), le quali devono costantemente essere sensibilizzate e formate sul rischio informatico. Nondimeno, un numero sufficiente di risorse umane (adeguatamente formato) deve essere dedicato alla raccolta di informazioni sulla vulnerabilità dei sistemi ICT aziendali e le sue possibili conseguenze (art. 13).

In aggiunta a quanto sopra, gli enti finanziari devono predisporre meccanismi idonei ad individuare automaticamente e tempestivamente le attività anomale, nonché "*punti di vulnerabilità (points of failure) importanti*" (art. 10).

Le entità finanziarie devono predisporre in anticipo "*piani di comunicazione delle crisi* [nds, che includano la comunicazione iniziale e gli aggiornamenti sui suoi sviluppi] *che consentano una divulgazione responsabile di informazioni riguardanti, almeno, gravi incidenti connessi alle TIC o vulnerabilità*" ai vari stakeholder (art. 14).

In occasione di incidenti ICT, gli enti finanziari devono esaminarne le cause integrando quanto è stato imparato dal fenomeno nel quadro per la gestione dei rischi informatici.

III. Gestione, classificazione e segnalazione degli incidenti informatici (artt. 17 – 23 DORA)

Con le norme in commento il Regolamento intende semplificare alcuni adempimenti già previsti dalla normativa vigente.

In particolare, le entità finanziarie dovranno predisporre un "*processo di gestione degli incidenti connessi alle TIC*" (art. 17), implementando piani di continuità operativa e di disaster recovery, nonché classificare e segnalare gli incidenti ICT, soprattutto quelli gravi (art. 19), all'Autorità competente. Il Regolamento non prevede scadenze temporali per la segnalazione rimettendo alle AEV l'adozione di standard tecnici entro 18 mesi dall'entrata in vigore della disciplina in commento.

Si rappresenta che le AEV dovranno emanare una relazione congiunta sulla fattibilità di un sistema centralizzato di segnalazione degli incidenti ICT (art. 21).

Il Regolamento, inoltre, all'art. 18, par. 2 stabilisce che le minacce informatiche si definiscono significative "*in base alla criticità dei servizi a rischio, comprese le operazioni dell'entità finanziaria, il numero e/o la rilevanza di clienti o controparti finanziarie interessati e l'estensione geografica delle aree a rischio*". Se, da un lato, la registrazione di tali minacce è obbligatoria, dall'altro, il DORA, coerentemente con quanto stabilito dalla direttiva 2016/1148/UE (c.d. direttiva

NIS), prevede che la notifica alle Autorità nazionali di vigilanza sia volontaria laddove le entità finanziarie "*ritengano che la minaccia sia rilevante per il sistema finanziario, gli utenti dei servizi o i clienti*" (art. 19).

IV. Test di resilienza operativa digitale (artt. 24 – 27 DORA).

Il Regolamento prevede che annualmente gli enti finanziari, diversi dalle microimprese, debbano sottoporre le proprie funzioni e servizi ICT critici e il proprio quadro di gestione dei rischi informatici a un test di resilienza operativa digitale "*solido ed esaustivo*" al fine di individuare le criticità dei propri sistemi e risolverle (art. 24).

In aggiunta a quanto sopra, le entità finanziare di rilevanti dimensioni, o che hanno un ruolo sistemico nel mercato finanziario, dovranno svolgere anche "*test di penetrazione basati su minacce, con cadenza almeno triennale*", c.d. *Thread-Led Penetration Testing* o TLPT (art. 26). Tali test devono riguardare almeno le funzioni e i servizi critici (art. 24).

I test devono essere svolti da soggetti, interni o esterni – quest'ultimi certificati dalle Autorità nazionali competenti -, indipendenti e con elevate competenze tecniche. In particolare, quelli incaricati di svolgere i test di penetrazione devono avere i requisiti di cui all'art. 27. Se i test sono svolti da un soggetto interno, le entità finanziarie dovranno dedicare risorse sufficienti a tale attività e garantiscono che siano evitati conflitti d'interessi durante le fasi di progettazione ed esecuzione del test. I test, inoltre, devono essere sempre improntati al principio di proporzionalità informante il Regolamento.

V. Gestione dei rischi informatici derivanti da terzi (artt. 28 – 44 DORA)

Il DORA dedica attenzione anche ai fornitori di servizi ICT critici i quali corrono i medesimi rischi delle entità finanziarie. Essi, pertanto, saranno assoggettati ad ampi poteri di supervisione e vigilanza delle AEV. Così quest'ultime potranno chiedergli di apportare modifiche alle proprie misure di sicurezza. Nondimeno, laddove ricorrano i requisiti stabiliti nel Regolamento, le AEV potranno imporre alle entità finanziarie di sospendere o risolvere i contratti con i propri fornitori di servizi ICT.

La normativa prevede anche delle condizioni contrattuali minime che gli operatori finanziari dovranno includere nei propri contratti con fornitori di servizi ICT al fine di garantire il rispetto delle previsioni del DORA.

Per quanto qui rileva, infine, bisogna precisare che il Regolamento rimette alla normativa secondaria, ossia i *Regulatory Technical Standard* o gli *Implementing Technical Standard*, da adottare a seconda dei casi entro 12 o 18 mesi dall'entrata in vigore del Regolamento, la regolazione di aspetti di dettagli del Regolamento stesso. Peraltro, la violazione delle disposizioni del DORA è sanzionabile dalle Autorità Europee di Vigilanza (artt. 50 ss. DORA).

L'art. 64 prevede che il Regolamento entri in vigore il ventesimo giorno successivo alla sua pubblicazione nella Gazzetta ufficiale dell'Unione europea e che si applichi a decorrere dal 17 gennaio 2023.

EMANUELE STABILE

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R2554&from=EN

4. Le modifiche apportate alla disciplina dell'abuso di dipendenza economica di cui alla legge sulla subfornitura, con decorrenza dal 31 ottobre 2022

Con decorrenza dal 31 ottobre 2022, l'art. 33 della legge 5 agosto 2022, n. 118 ha modificato la disciplina dell'abuso di dipendenza economica contenuta nella legge sulla subfornitura (art. 9 della legge 18 giugno 1998, n. 192 recante la disciplina della subfornitura nelle attività produttive: di seguito "**l. subfornitura**"), disponendo due integrazioni di diritto sostanziale riguardanti le piattaforme digitali, e una modifica generale (ossia non limitata ai rapporti riguardanti le piattaforme digitali) sulla competenza giurisdizionale.

La prima integrazione riguarda la nozione di dipendenza economica. Come noto, la dipendenza economica non è di per sé vietata dalla l. subfornitura, essendone invece vietato l'abuso. Interessante appare la formulazione della norma che richiede di guardare agli "effetti di rete" e alla "disponibilità dei dati" per stabilire se possa dirsi che una piattaforma digitale abbia o meno un "ruolo determinante per raggiungere utenti finali o fornitori" dell'impresa di cui importi predicare una situazione di dipendenza economica dalla medesima piattaforma digitale. La seconda integrazione riguarda per l'appunto l'abuso di dipendenza economica. La norma prevede come figure sintomatiche di abuso di dipendenza economica pratiche informative ingannevoli (commissive od omissive) relativamente al servizio erogato dalla piattaforma digitale, oppure pratiche della piattaforma digitale che consistono nel pretendere dall'impresa prestazioni ingiustificate ovvero

nell'ostacolare il ricorso da parte di quest'ultima a fornitori diversi. Con la terza modifica è stata disposta la competenza delle sezioni specializzate in materia di impresa per le controversie di abuso di dipendenza economica ai sensi della l. subfornitura. È una modifica di cui si avvertiva l'esigenza da tempo, a prescindere dai rapporti concernenti le piattaforme digitali.

In particolare:

- al primo comma dell'art. 9 l. subfornitura è stato aggiunto, in fine, il seguente periodo «*Salvo prova contraria, si presume la dipendenza economica nel caso in cui un'impresa utilizzi i servizi di intermediazione forniti da una piattaforma digitale che ha un ruolo determinante per raggiungere utenti finali o fornitori, anche in termini di effetti di rete o di disponibilità dei dati*»;
- al secondo comma dell'art. 9 l. subfornitura è stato aggiunto, in fine, il seguente periodo: «*Le pratiche abusive realizzate dalle piattaforme digitali di cui al comma 1 possono consistere anche nel fornire informazioni o dati insufficienti in merito all'ambito o alla qualità del servizio erogato e nel richiedere indebite prestazioni unilaterali non giustificate dalla natura o dal contenuto dell'attività svolta, ovvero nell'adottare pratiche che inibiscono od ostacolano l'utilizzo di diverso fornitore per il medesimo servizio, anche attraverso l'applicazione di condizioni unilaterali o costi aggiuntivi non previsti dagli accordi contrattuali o dalle licenze in essere*»
- al terzo comma dell'art. 9 l. subfornitura è stato aggiunto, in fine, il seguente periodo: «*Le azioni civili esperibili a norma del presente articolo sono proposte di fronte alle sezioni specializzate in materia di impresa di cui all'articolo 1 del decreto legislativo 27 giugno 2003, n. 16*»

Si tratta di modifiche importanti per una legge importante. Sembra opportuno sottolineare che la l. subfornitura del 1998 è interamente italiana: non fu emanata in attuazione di alcuna direttiva europea e non ha ricalcato modelli evidenti di legislazione di altri Stati membri dell'UE. Come può vedersi, essa ha invece anticipato molti temi oggi all'attenzione del diritto dell'Unione europea.

SALVATORE ORLANDO

https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1998;192%7Eart9

5. La EU Interinstitutional declaration on digital rights and principles del 14.11.2022

Lo scorso 14 novembre 2022 il Consiglio dell'Unione europea ha annunciato, mediante un comunicato stampa, che si sono conclusi i negoziati tra gli Stati membri, il Parlamento e la Commissione per la stesura di una *interistitutional* "*European declaration on digital rights and principles for the digital decade*" ("*Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*", la "**Dichiarazione**").

A seguito della conclusione dei negoziati, Ivan Bartoš – vice Primo Ministro per la Digitalizzazione e Ministro per lo Sviluppo regionale della Repubblica Ceca (e cioè dello Stato membro che, sino al 31 dicembre 2022, presiede il Consiglio dell'UE) – ha annunciato che "*la Dichiarazione definisce una via europea per la trasformazione digitale delle nostre società ed economie*" posto che "*è essenziale promuovere e proteggere i nostri valori nell'ambiente digitale, che si tratti di privacy, controllo individuale sui dati, parità di accesso ai servizi e all'istruzione, condizioni di lavoro giuste ed eque, impegno nello spazio pubblico o libertà di scelta*". L'augurio (o, come anche si suole dire, la *mission*) delle istituzioni europee è che "*la dichiarazione costituisca un punto di riferimento internazionale e ispiri altri Paesi e organizzazioni a seguire il nostro esempio*".

La Dichiarazione – il cui testo definitivo non è ancora disponibile – prende le mosse dalla proposta adottata dalla Commissione il 26 gennaio 2022 (nel contesto della *2030 Digital Compass*: https://futurium.ec.europa.eu/en/digital-compass), la quale si articola in 6 "capitoli" che si pongono l'obiettivo di promuovere i valori europei nell'ambito della trasformazione digitale:

1. ponendo in primo piano le persone e i loro diritti;
2. sostenendo la solidarietà e l'inclusione;
3. garantendo la libertà di scelta online;
4. promuovendo la partecipazione allo spazio pubblico digitale;
5. aumentando la sicurezza, la protezione e la responsabilizzazione delle persone;
6. promuovendo la sostenibilità del futuro digitale;

il tutto facendo sì che la tecnologia digitale sia rivolta a beneficio di tutti gli individui e le imprese nonché della società nel suo complesso.

Il primo capitolo della Dichiarazione – finalizzato, come detto, a "*mettere le persone al centro della trasformazione digitale*" ponendo la tecnologia "*al servizio* […] *e a beneficio di tutti gli europei*" per "*metterli nelle condizioni di perseguire le loro aspirazioni, in tutta sicurezza e nel rispetto dei loro diritti fondamentali*" – pone l'impegno delle istituzioni europee a "*rafforzare il quadro democratico per una trasformazione digitale che vada a beneficio di ogni persona e migliori la vita di tutti gli europei*", "*adottare le misure necessarie per garantire che i valori dell'Unione e i diritti delle persone riconosciuti dal diritto dell'Unione siano rispettati online così come offline*", "*promuovere un'azione responsabile e diligente da parte di tutti gli attori digitali, pubblici e privati, per un ambiente digitale sicuro e protetto*" e "*promuovere attivamente questa visione della trasformazione digitale, anche nelle relazioni internazionali*".

Il secondo capitolo, finalizzato alla promozione della "*solidarietà*" e della "*inclusione*", racchiude l'impegno delle istituzioni europee a "*garantire che le soluzioni tecnologiche rispettino i diritti delle persone, consentano l'esercizio di tali diritti e promuovano l'inclusione*", "*perseguire una trasformazione digitale che non lasci indietro nessuno, che includa in particolare gli anziani, le persone con disabilità, le persone emarginate, vulnerabili o prive di diritti, così come coloro che agiscono per loro conto*" e "*sviluppare quadri adeguati affinché tutti gli operatori del mercato che traggono vantaggio dalla trasformazione digitale si assumano le proprie responsabilità sociali e contribuiscano in modo equo e proporzionato ai costi delle infrastrutture, dei servizi e dei beni pubblici, a beneficio di tutti gli europei*". In questo contesto, l'obiettivo europeo è quello di garantire i diritti di "*ogni persona*" a un "*accesso alla connettività digitale ad alta velocità a prezzi accessibili*", nonché "*all'istruzione, alla formazione e all'apprendimento permanente*" finalizzato ad "*acquisire tutte le competenze digitali di base e avanzate*", ad avere "*condizioni di lavoro eque, giuste sane e* sicure" e "*una protezione adeguata nell'ambiente digitale come nel luogo di lavoro fisico*", oltre all'"*accesso a tutti i servizi pubblici principali online in tutta l'Unione*".

Il terzo capitolo della Dichiarazione, dedicato alla "*libertà di scelta*", contiene l'impegno delle istituzioni europee a far sì che "*ogni persona*" sia "*messa nelle condizioni di godere dei benefici offerti dall'intelligenza artificiale facendo le proprie scelte informate nell'ambiente digitale, e rimanendo al contempo protetta dai rischi e dai danni alla salute, alla sicurezza e ai diritti fondamentali*" e possa "*essere in grado di scegliere realmente quali servizi online utilizzare, sulla base di informazioni obiettive, trasparenti e affidabili*", nonché di "*competere lealmente e innovare nell'ambiente digitale*".

Alla "*partecipazione allo spazio pubblico digitale*" è dedicato il quarto capitolo della Dichiarazione, con cui le istituzioni si impegnano a: "*sostenere lo sviluppo e l'utilizzo ottimale delle tecnologie digitali per stimolare il coinvolgimento dei cittadini e la partecipazione democratica*", "*continuare a salvaguardare i diritti fondamentali online, in particolare la libertà di espressione e di informazione*", "*adottare misure volte a contrastare tutte le forme di contenuti illegali proporzionatamente al danno che possono causare e nel pieno rispetto del diritto alla libertà di espressione e di informazione, senza imporre obblighi generali di sorveglianza*" e "*creare un ambiente online in cui le persone siano protette dalla disinformazione e da altre forme di contenuti dannosi*".

Il quinto capitolo contiene invece l'impegno istituzionale alla creazione di "*un ambiente online sicuro e protetto*", alla "*protezione dei propri dati personali online*" nonché "*alla riservatezza delle proprie comunicazioni e delle informazioni*". Esso contiene altresì alcuni impegni volti a garantire protezione, autonomia e responsabilità per "*i bambini e i giovani*".

Il sesto capitolo – sulla "*sostenibilità*" – contiene, infine, l'impegno a "*favorire lo sviluppo e l'utilizzo di tecnologie digitali sostenibili che abbiano un impatto ambientale e sociale minimo*" e a "*sviluppare e diffondere soluzioni digitali con ricadute positive per l'ambiente e il clima*".

L'esito dei negoziati è ora soggetto all'approvazione del Consiglio, del Parlamento europeo e della stessa Commissione. Per quanto riguarda il Consiglio, la presidenza ceca intende sottoporre l'accordo ai rappresentanti degli Stati membri (COREPER) il prima possibile per consentirne la firma da parte delle tre istituzioni cofirmatarie durante il Consiglio europeo di dicembre.

RICCARDO ALFONSI

https://www.consilium.europa.eu/en/press/press-releases/2022/11/14/declaration-on-digital-rights-and-principles-eu-values-and-citizens-at-the-centre-of-digital-transformation/

https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration

6. Il codice deontologico "rafforzato" del 2022 di buone pratiche contro la disinformazione.

Lo scorso 16 giugno 2022 è stato presentato il codice rafforzato di buone pratiche sulla disinformazione ("codice rafforzato", in inglese *2022 Strengthened Code of Practice on Disinformation*), firmato da 34 soggetti operanti nel settore (piattaforme *online*, rappresentanti della società civile, della pubblicità, della ricerca, associazioni di categoria, etc.). Il codice rafforzato rappresenta il tentativo di aggiornare il codice di buone pratiche sulla disinformazione approvato nel 2018 ("codice 2018", in inglese: *Code of Practice on Disinformation*) alle indicazioni provenienti dalla Commissione europea, che nel maggio 2021 aveva fornito delle linee guide ("*Guidance*"), e dal lungo processo di revisione e monitoraggio avviato autonomamente dai diversi soggetti firmatari.

Tale processo era iniziato nel gennaio del 2019, quando i firmatari avevano pubblicato una prima relazione sull'implementazione degli impegni assunti nel codice 2018. Nell'ottobre dello stesso anno, gli stessi firmatari avevano presentato un interessante report di autovalutazione che restituiva i vari progressi effettuati dalle piattaforme e dagli inserzionisti. Nel settembre 2020 la Commissione europea aveva reso pubblica la sua prima valutazione del codice 2018, riconoscendo che gli impegni assunti avevano garantito una maggiore trasparenza e partecipazione delle piattaforme nella lotta alla disinformazione. La stessa valutazione indicava diversi punti critici del codice 2018, primo fra tutti il mancato accesso ai dati per una valutazione terza e indipendente circa il fenomeno della disinformazione in rete.

Il 26 maggio 2021, anche sulla scorta di quanto emerso in relazione alla disinformazione online in tempi di pandemia Covid-19, la Commissione ha così pubblicato le *Guidance*, indicando come il codice 2018 andrebbe migliorato. Sviluppando i rilievi presentati l'anno precedente, le *Guidance* insistono sulla necessità di migliorare l'accesso ai dati, di creare un miglior monitoraggio del fenomeno e di responsabilizzare maggiormente gli utenti dei servizi dell'informazione. Grande importanza era riconosciuta alla c.d. *Demonetising disinformation*, ossia alla riduzione della diffusione di disinformazione sui servizi dei firmatari o su siti web di terzi tramite l'impegno a non inserire della pubblicità accanto a contenuti di disinformazione o in luoghi noti per la pubblicazione ripetuta di disinformazione. Orbene, il recente codice rafforzato recepisce tutte queste indicazioni, innova il testo originario e aumenta il numero di soggetti coinvolti.

Per quanto concerne l'oggetto, il codice rafforzato fa riferimento alla disinformazione come definita dalla Commissione europea nella Comunicazione sull'*European Democracy Action Plan* del 3 dicembre 2020, COM(2020) 790 final (su cui v. la notizia n. 1 nel numero 1/2021 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio.pdf), ripetendone le varie accezioni di cattiva informazione ("contenuti falsi o fuorvianti, condivisi senza intenzione fraudolenta, anche se gli effetti possono comunque essere dannosi, ad esempio quando le persone condividono informazioni false con amici e familiari in buona fede"), disinformazione ("contenuto falso o fuorviante, diffuso con l'intento di ingannare o ottenere un guadagno economico e che può provocare danni pubblici"), influenza delle informazioni ("sforzi coordinati da parte di soggetti nazionali o esterni volti a influenzare il pubblico destinatario utilizzando una serie di mezzi ingannevoli, tra cui la soppressione di fonti di informazione indipendenti in combinazione con la disinformazione") e di ingerenze straniere nello spazio informativo ("misure coercitive e ingannevoli impiegate da un soggetto statale straniero o dai suoi agenti per ostacolare la libertà di informazione e di espressione della volontà politica degli individui").

Il codice rafforzato si compone di un preambolo e di sette sezioni, in cui si affermano 44 impegni (*commitment*). Rispetto a molti di questi impegni assunti dai firmatari, il codice prevede anche delle pratiche attuative (*measures*) ed offre indicazioni concrete. La sezione sul controllo delle inserzioni pubblicitarie ("*scrutiny of ad placements*") racchiude impegni importanti come quello a evitare l'uso di sistemi pubblicitari per diffondere, sotto forma di messaggi pubblicitari, della disinformazione. La sezione successiva si occupa del tema dei messaggi pubblicitari politici e riflette le osservazioni che la Commissione e gli stessi firmatari hanno ricavato dall'osservazione delle ultime elezioni europee. È interessante notare che il codice rafforzato non offre una specifica definizione di *political advertising*, preferendo richiamare quella contenuta nella proposta di regolamento relativo alla trasparenza e al targeting della

pubblicità politica (art. 2.1, 2: "la preparazione, collocazione, promozione, pubblicazione o diffusione, con qualsiasi mezzo, di un messaggio: a) di, a favore o per conto di un attore politico, salvo se di natura meramente privata o meramente commerciale; oppure b)che possa influenzare l'esito di un'elezione o di un referendum, di un processo legislativo o regolamentare o di un comportamento di voto") (su questa proposta v. la notizia n. 6 nel numero 1/2022 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf). Non dovesse tale proposta di regolamento sulla pubblicità politica essere approvata nel primo anno di vigenza del codice rafforzato, i firmatari del codice rafforzato si impegnano ad affidare a una task-force l'elaborazione di una definizione analoga. La sezione sull'integrità dei servizi contiene tre raccomandazioni, tra cui quella propria dei fornitori di sistemi di intelligenza artificiale e che diffondono contenuti generati e manipolati dall'IA attraverso i loro servizi (es. *deepfakes*) a prendere in considerazione gli obblighi di trasparenza e l'elenco delle pratiche manipolative di cui alla proposta di regolamento sull'intelligenza artificiale (su cui v. la notizia n. 1 nel numero 1/2021 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio-1.pdf). La sezione "*empowering users*" presenta numerosi impegni, tra cui quello a ridurre al minimo i rischi di propagazione virale di contenuti di disinformazione tramite l'adozione di pratiche di progettazione sicure nello sviluppo. La sezione "*empowering the research community*" disciplina, tra le altre cose, l'accesso automatizzato (es. API) e l'utilizzo per finalità di ricerca dei dati non personali, anonimizzati, aggregati o già pubblici. Un significativo impegno a dialogare e coinvolgere specifici soggetti è previsto nella sezione "*Empowering the fact-checking community*"; qui, ad esempio al *commitment* 31, si afferma l'impegno a integrare, mettere in mostra o comunque utilizzare in modo coerente il lavoro dei *fact-checkers* nei servizi offerti dalle varie piattaforme che hanno sottoscritto il codice rafforzato. Le sezioni finali contengono impegni relativi alla trasparenza circa l'implementazione del codice rafforzato, all'istituzione di una task-force *ad hoc* e al continuo monitoraggio dello stesso codice, in vista di un suo futuro aggiornamento. Tra i firmatari figurano Adobe, Associazione europea delle agenzie di comunicazione (EACA), Google, IAB Europe (Interactive Advertising Bureau Europe), Meta, Microsoft, Reporter senza frontiere (RSF), TikTok, Twitch, Twitter, Vimeo e Federazione mondiale degli inserzionisti (WFA). Ciascuno di essi ha firmato gli impegni in un documento, pubblicamente accessibile, che prevede le misure pertinenti per i propri servizi.

DANIELE IMBRUGLIA

https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

https://digital-strategy.ec.europa.eu/it/library/2022-strengthened-code-practice-disinformation

7. L'opinion del 16.9.2022 della United States Court of Appeals for the Fifth Circuit nella causa contro la legge del Texas HB20 (NetChoice LLC v. Paxton): libertà di parola versus moderazione di contenuti da parte delle piattaforme online

Il 16 settembre 2022 la *United States Court of Appeals for the Fifth Circuit* è intervenuta nel caso *NetChoice LLC v. Paxton* riguardante uno Statuto del Texas, denominato *House Bill 20* (di seguito anche *"***HB20***"*), che, come la stessa Corte afferma "*generally prohibits large social media platforms from censoring speech based on the viewpoint of its speaker*".

L'*House Bill 20*, emanato il 9 settembre 2021, regola le piattaforme con oltre cinquanta milioni di utenti attivi al mese, definendole come un sito internet o un'applicazione aperta al pubblico che consente ad un utente di creare un *account* e comunicare con altri utenti allo scopo principale di pubblicare informazioni, commenti, messaggi o immagini.

HB20 è stato al centro di un dibattito che ha visto contrapporsi la posizione delle grandi piattaforme a quella dello Stato federale del Texas tra diverse vicende giudiziarie.

NetChoice LLC (NetChoice) e Computer & Communications Industry Association (CCIA), che rappresentano le aziende che operano come piattaforme digitali, hanno citato in giudizio il procuratore generale del Texas (Mr. Ken Paxton) prima che l'*House Bill 20* entrasse in vigore. A seguito di ciò, il Tribunale distrettuale ne ha disposto la sospensione temporanea sostenendo l'illegittimità costituzionale di alcune disposizioni ivi contenute.

La pronuncia del 16 settembre 2022 della *United States Court of Appeals for the Fifth Circuit* (di seguito anche la "**Opinion**") ha ribaltato la decisione del Tribunale distrettuale.

NetChoice e CCIA ritengono che HB20 sia incostituzionale in quanto contrario al Primo Emendamento della Costituzione degli Stati Uniti d'America, ai sensi del quale «*il Congresso non potrà porre in essere leggi per il riconoscimento ufficiale di una religione o per proibirne il libero culto, per limitare la libertà di parola o di stampa o che limitino il diritto della gente a riunirsi in forma pacifica e a presentare petizioni al governo per riparare alle ingiustizie*».

NetChoice e CCIA affermano che la libertà di parola delle piattaforme sia violata se non è consentito alle stesse di censurare i contenuti che per il loro tramite sono diffusi. La *Court of Appeals, 5th Circuit* sostiene che gli argomenti a tutela di un preteso diritto di censura delle piattaforme sono "*staggering*" e che "*the platforms offer a rather odd inversion of the First Amendment. That Amendment, of course, protects every person's right to 'the freedom of speech.' But the platforms argue that buried somewhere in the person's enumerated right to free speech lies a corporation's unenumerated right to muzzle speech*".

La *United States Court of Appeals for the Fifth Circuit* evidenzia che due sezioni del *Texas House Bill 20* vengono in rilievo nel caso di specie. La prima è la Sezione 7, che riguarda la censura dei post degli utenti e prevede, in via generale, che "*a social media platform may not censor a user, a user's expression, or a user's ability to receive the expression of another person based on the viewpoint of the user or another person; the viewpoint represented in the user's expression or another person's expression; or a user's geographic location in this state or any part of this state*".

La Sezione 7 non esclude, anzi consente espressamente che sia rimossa ogni espressione che sia "*the subject of a referral or request from an organization with the purpose of preventing the sexual exploitation of children and protecting survivors of sexual abuse from ongoing harassment*", oppure che "*directly incites criminal activity or consists of specific threats of violence targeted against a person or group because of their race, color, disability, religion, national origin or ancestry, age, sex, or status as a peace officer or judge*"; o che sia una "*unlawful expression*".

La United *States Court of Appeals for the Fifth Circuit* approda ad esiti completamente diversi da quelli sperati dalle grandi piattaforme ed è chiara nel rigettare l'idea che le piattaforme abbiano ‹‹*a freewheeling First Amendment right to censor what people say*››. Nello specifico la Corte d'Appello afferma che non si può richiamare il Primo Emendamento a tutela di un presunto diritto di censura da parte delle piattaforme, visto che riconoscere tale diritto significherebbe non tutelare proprio la libertà di parola garantita dal Primo Emendamento. Non si può, in altri termini, ribaltare il Primo Emendamento, consentendo alle piattaforme di invocarlo per limitare, attraverso un loro presunto diritto alla censura, la libertà di parola degli altri. Nemmeno si può temere che il rifiuto di considerare incostituzionali il *Texas House Bill 20* inibisca la libera manifestazione del proprio pensiero o scoraggi commenti su questioni di interesse pubblico.

Per *la United States Court of Appeals for the Fifth Circuit* la libertà di parola non implica il diritto di censura e, comunque, la Sezione 7 del *Texas House Bill 20* non limita la libertà di parola delle piattaforme. Tanto è vero che, sostiene la Corte, a p. 34 della Opinion: ‹‹*no category of Platform speech can trigger any additional duty—or obviate an existing duty—under Section 7. And Section 7 does not create a special privilege for those who disagree with the Platforms' views (...). Rather, it gives the exact same protection to all Platform users regardless of their viewpoint*››.

La Sezione 2 del *Texas House Bill 20* impone dettagliati requisiti che le piattaforme devono rispettare nello svolgere l'attività di moderazione. Segnatamente, le piattaforme devono ‹‹*disclose how they moderate and promote content and publish an "acceptable use policy"*››; descrivere come gli utenti possono notificare alle stesse piattaforme i contenuti che si pongono in contrasto con detta politica, prevedere un sistema di reclamo e ricorso per i propri utenti e pubblicare un "*biannual transparency report*".

Il Tribunale distrettuale, sposando di fatto le ragioni delle grandi piattaforme, considera incostituzionale la Sezione 2 del *Texas House Bill 20* per diverse ragioni. Prima di tutto, ritiene che siano imposti alle piattaforme obblighi considerati eccessivamente gravosi in ragione dell'elevato numero di messaggi che transitano sui siti *web.* Inoltre, il Tribunale afferma che le ‹‹*social media platforms are not common carriers*›› e che la gestione e organizzazione dei contenuti rientri nella discrezionalità editoriale delle piattaforme. In base a questa impostazione la ‹‹*prohibition on viewpoint-based censorship*›› violerebbe la discrezionalità editoriale delle piattaforme. Anche quest'ultima, a detta delle piattaforme, sarebbe protetta dal Primo Emendamento. In merito, la *United States Court of Appeals for the Fifth Circuit* dimostra tutto il suo disappunto, evidenziando che è contraddittorio l'atteggiamento delle piattaforme che invocano la

discrezionalità editoriale degli editori, pur non volendo assumersi le relative responsabilità. Le piattaforme, infatti, rivendicano il loro ruolo di intermediari di contenuti riferibili ad altri e dalle stesse difficilmente controllabili, anche in ragione del numero elevato di post che consentono di pubblicare. Il dato spiega il ricorso delle piattaforme agli algoritmi per escludere determinati contenuti e la diversità del controllo effettuato rispetto al classico giudizio editoriale tipico dei giornali.

La *United States Court of Appeals for the Fifth Circuit* ribadisce che ‹‹*editorial discretion involves "selection and presentation" of content before that content is hosted, published, or disseminated. The Platforms do not choose or*

select material before transmitting it. They engage in viewpoint-based censorship with respect to a tiny fraction of the expression they have already disseminated››.

La *United States Court of Appeals for the Fifth Circuit* esclude convintamente l'equiparabilità delle piattaforme ai giornali anche richiamando i termini e le condizioni del servizio di alcune tra le più grandi piattaforme (Twitter, Terms of Service, https://twitter.com/en/tos; Facebook, Terms of Service, https://www.facebook.com/terms.php). Ivi le stesse affermano che non esprimono un giudizio editoriale e non possono assumersi la responsabilità dei contenuti, ma sono soltanto canali attraverso i quali transitano discorsi di altri.

A differenza di giornali invocati dalle piattaforme per analogia, sulle piattaforme digitali sono, tra l'altro, praticamente inesistenti vincoli di spazio, così che le stesse possono ospitare il discorso degli utenti senza rinunciare al loro potere o al loro diritto di esprimere eventualmente la propria opinione in merito, anche prendendo le distanze dal messaggio che ospitano.

Altro aspetto di particolare interesse in *NetChoice, LLC, v. Paxton*, n. 21-51178 è l'attenzione ai rischi di discriminazione e ai paradossi che possono verificarsi.

Ad ulteriore sostegno dell'incostituzionalità del *Texas House Bill 20*, il Tribunale distrettuale ritiene che si tratti di una legge discriminatoria sia dal punto di vista oggettivo, sia dal punto di vista soggettivo. Quanto a quest'ultimo aspetto la discriminazione è individuata nel fatto che il *Texas House Bill 20* si applica solo alle grandi piattaforme. Dal punto di vista oggettivo, invece, il *Texas House Bill 20* è considerata una legge discriminatoria in quanto consente di censurare soltanto alcuni tipi di contenuti indicati in modo specifico.

La *United States Court of Appeals for the Fifth Circuit* dimostra che a poter essere discriminatorio non è quanto previsto dal *Texas House Bill 20*, ma piuttosto un potere indiscriminato delle piattaforme di censurare i contenuti in base al loro punto di vista. Il *Texas House Bill 20* limita e regolamenta il potere delle piattaforme di rimuovere i contenuti proprio per evitare la discriminazione e garantire la stessa protezione a tutti gli utenti della piattaforma, indipendentemente dal loro punto di vista.

SARA TOMMASI

https://www.ca5.uscourts.gov/opinions/pub/21/21-51178-CV1.pdf

8. La sentenza CGUE del 20.10.2022 nella causa C-77/21 sui principî di limitazione delle finalità e di limitazione della conservazione ex art. 5 lett. b) ed e) GDPR

Il 20 ottobre 2022 la Corte di Giustizia dell'Unione Europea ("CGUE" o la "Corte") si è pronunciata nella causa C-77/21 sulla portata dei principi di limitazione delle finalità e limitazione della conservazione, enunciati rispettivamente dall'art. 5, par. 1, lett. *b)* ed *e)* del Regolamento (UE) 2016/679 (GDPR).

La Corte si è pronunciata sulla domanda pregiudiziale sollevata dalla Corte di Budapest nell'ambito di una controversia tra uno dei principali fornitori di servizi Internet e di telediffusione dell'Ungheria (Digi Távközlési és Szolgáltató Kft., di seguito la "Digi") e l'autorità ungherese per la protezione dei dati e della libertà d'informazione.

La controversia nasceva dal fatto che, a seguito di un guasto tecnico che aveva interessato il funzionamento di un server, la Digi aveva creato una banca dati di test in cui aveva copiato i dati personali di circa un terzo dei clienti abbonati alla sua newsletter, dati che erano stati originariamente raccolti ai fini della conclusione e dell'esecuzione dei contratti di abbonamento. Successivamente, dopo aver effettuato i test necessari e aver corretto l'errore, la Digi non aveva soppresso la banca dati di test, per cui i dati personali erano rimasti conservati in tale banca dati per quasi 18 mesi, finché la stessa non era stata oggetto di un attacco *hacker*.

La Corte ungherese ha sollevato davanti alla CGUE due questioni: (i) se il principio della limitazione della finalità previsto dall'art. 5, par. 1, lett. *b)* GDPR impedisca la registrazione e la conservazione, in una banca dati creata al fine di effettuare test e di correggere errori, di dati

personali precedentemente raccolti e conservati in un'altra banca dati; e (ii) se sia compatibile con il principio della limitazione della conservazione di cui all'art. 5, para. 1, lett. *e)* GDPR il fatto che il titolare del trattamento conservi in un'altra banca dati alcuni dati personali che sono stati raccolti e conservati per una finalità legittima limitata.

Con riferimento alla prima questione, la CGUE ha rilevato che nel caso di specie i dati personali erano stati raccolti per finalità determinate, esplicite e legittime, ovvero la conclusione e l'esecuzione da parte della Digi di contratti di abbonamento con i suoi clienti. Pertanto, la registrazione e la conservazione di tali dati nella banca dati di test costituisce un trattamento ulteriore che, ai sensi dell'art. 5, par. 1, lett. *b)* GDPR in combinato disposto con l'art. 6, par. 4 GDPR, deve essere compatibile con le finalità per le quali i dati sono stati inizialmente raccolti. In particolare, quando il trattamento ulteriore non è basato sul consenso o su un atto legislativo, la valutazione di compatibilità con la finalità originaria deve tener conto, tra l'altro, dell'eventuale nesso tra le finalità, del contesto in cui i dati sono stati raccolti, della natura dei dati personali, delle possibili conseguenze dell'ulteriore trattamento per gli interessati e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento. Nello specifico, deve esserci un nesso concreto, logico e sufficientemente stretto tra le finalità della raccolta iniziale dei dati e l'ulteriore trattamento, tale da garantire che tale ulteriore trattamento non si discosti dalle legittime aspettative degli interessati.

Nel caso di specie, la CGUE ha rilevato che il principio di limitazione delle finalità non impedisce la realizzazione di test e la correzione di errori sulla banca dati degli abbonati, in quanto tali finalità presentano un nesso concreto con l'esecuzione dei contratti di abbonamento. Eventuali errori potrebbero infatti impedire la corretta fornitura del servizio contrattualmente previsto e per cui i dati sono stati inizialmente raccolti. Tali trattamenti, pertanto, non si discostano dalle legittime aspettative degli interessati, ferma restando la necessità di verificare in concreto l'eventuale presenza di dati sensibili, il rischio di conseguenze dannose per gli abbonati e la presenza di garanzie adeguate.

Con riferimento alla seconda questione, la CGUE ha ricordato innanzitutto che, ai sensi dell'art. 5, par. 1, lett. e) GDPR, i dati personali devono essere conservati per un periodo non superiore a quanto necessario al conseguimento delle finalità per le quali sono stati raccolti o sono stati ulteriormente trattati. Ne consegue che anche un trattamento inizialmente lecito può diventare illecito se i dati non sono più necessari al conseguimento delle finalità previste. La Corte ha concluso, dunque, che nel caso di specie rappresenta una violazione del principio di limitazione della conservazione non aver cancellato i dati personali degli interessati dalla banca dati di test immediatamente dopo la realizzazione dei test e la correzione degli errori.

CHIARA RAUCCIO

https://curia.europa.eu/juris/document/document.jsf;jsessionid=9FCFA1A51DE86902447C21968565D067?text=&docid=267405&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=237767

9. La sentenza CGUE del 27.10.2022 nella causa C-129/21 Proximus (Annuaires électroniques publics) sulle misure da adottarsi da parte del titolare del trattamento di dati personali per informare i motori di ricerca in Internet di una richiesta di cancellazione rivoltagli dall'interessato.

Il 27 ottobre 2022 la Corte di Giustizia dell'Unione Europea (CGUE) si è espressa su una vicenda che trae origine dalle operazioni di trattamento di dati personali effettuate da Proximus NV (Proximus), fornitore di servizi di telecomunicazione in Belgio il quale, in particolare, offre un servizio di accesso e trasmissione di elenchi telefonici contenenti il nome, l'indirizzo e il numero di telefono degli abbonati. Tali dati, salvo i casi in cui l'interessato non abbia esplicitato una volontà contraria (cd. *opt out*), vengono comunicati da altri operatori a Proximus, la quale, a sua volta, li trasmette a nuovi fornitori.

Il reclamante è un abbonato di uno di tali servizi, Telenet, operatore che trasmette proprio i suddetti dati di contatto a Proximus. L'interessato ha richiesto di non far comparire tali informazioni negli elenchi telefonici pubblicati da quest'ultima società, nonchè da terzi. In seguito a questa richiesta Proximus ha registrato l'*opt out* e provveduto affinchè i dati del reclamante non venissero più resi pubblici. Successivamente, tuttavia, Proximus ha ricevuto da Telenet una nuova comunicazione dei dati in questione e, non essendo stata riscontrata dai sistemi di Proximus l'opposizione dell'interessato, le informazioni sono state nuovamente pubblicate da Proximus.

In risposta alle successive e ripetute richieste dell'abbonato di non inserire i suoi dati, Proximus ha poi dichiarato di aver ritirato i dati in questione dagli elenchi e di aver contattato Google per far cancellare i relativi *link* al sito *web* di Proximus, informando inoltre l'abbonato di aver notificato agli altri fornitori a cui i dati erano stati comunicati la richiesta di rimozione dei dati dai registri pubblici.

L'interessato ha inoltre presentato un reclamo all'Autorità belga per la protezione dei dati (Gegevensbeschermingsautoriteit), la quale ha inflitto a Proximus una sanzione di ventimila euro per violazione degli articoli 5, par. 2, 6, 7 e 24 del Regolamento (UE) 2016/679 (GDPR). L'Autorità ha inoltre ordinato a Proximus di dare immediato seguito alla revoca del consenso e di conformarsi alle richieste del reclamante volte all'esercizio del suo diritto alla cancellazione dei dati personali. Infine, ha intimato a Proximus di cessare di comunicare illecitamente tali dati ad altri fornitori di elenchi telefonici.

Proximus ha impugnato il provvedimento presso la Corte d'appello di Bruxelles che, in virtù delle questioni interpretative emergenti nel caso concreto, ha sollevato la questione pregiudiziale nei confronti della CGUE.

Nello specifico, Proximus riteneva che, sulla base dell'articolo 45, paragrafo 3 della Direttiva (UE) 2002/58 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche ("direttiva ePrivacy"), non è necessario un consenso dell'abbonato alla pubblicazione dei suoi dati sugli elenchi telefonici, bensì sono gli abbonati stessi che devono chiedere di non figurarvi, secondo il suindicato sistema di *opt out*.

Su tale questione, la CGUE, facendo riferimento all'articolo 12, paragrafo 2, della direttiva ePrivacy afferma che il consenso dell'abbonato di un operatore di servizi telefonici è necessario affinché i dati personali di tale interessato siano inclusi nei relativi elenchi, pubblicati da fornitori diversi da tale operatore. Il consenso in questione, allo stato attuale e in assenza di ulteriori e più specifiche indicazioni normative, deve rispettare i requisiti dell'articolo 4, punto 11 del GDPR e può, in ogni caso, essere raccolto da detto operatore o da uno di tali fornitori. Tale consenso, secondo la CGUE si estende a qualsiasi trattamento ulteriore dei dati da parte di imprese terze attive nel mercato dei servizi di consultazione degli elenchi telefonici accessibili al pubblico, sempre che tali trattamenti perseguano lo "stesso scopo" e, dunque, non siano effettuati per finalità non compatibili con quella originaria.

Con la seconda e la quarta questione, il giudice del rinvio si è soffermato sulla natura dell'articolo 17 del GDPR che disciplina il cd. "diritto alla cancellazione" dei dati personali.

In particolare, la Corte d'Appello ha chiesto se tale disposizione debba essere interpretata nel senso che la richiesta di un abbonato diretta all'eliminazione delle sue informazioni dagli elenchi configuri l'esercizio di tale diritto e comporti, pertanto, la cancellazione dei dati personali del richiedente e non la sola rimozione degli stessi dagli elenchi con relativa modifica dello status del reclamante a soggetto che si oppone alla pubblicazione delle proprie informazioni, così come operata da Proximus. È stato inoltre richiesto dal giudice del rinvio se l'articolo 17, paragrafo 2 del GDPR consenta a un'Autorità di controllo nazionale di ordinare a un fornitore di elenchi telefonici, al quale l'abbonato ha chiesto di non pubblicare più i dati personali che lo riguardano, di adottare «misure ragionevoli», ai sensi di tale disposizione, al fine di informare i gestori dei motori di ricerca di tale domanda di cancellazione dei dati.

Su entrambe le questioni, la CGUE ha adottato un'interpretazione non in contrasto con quella dell'Autorità di controllo belga, ritenendo che l'articolo 17 del GDPR deve essere interpretato nel senso che la richiesta di un abbonato diretta all'eliminazione dei suoi dati personali dagli elenchi telefonici costituisce un esercizio del diritto alla cancellazione e che il paragrafo 2 del medesimo articolo consente a un'autorità di controllo nazionale di ordinare a un fornitore di elenchi telefonici, in seguito a relativa richiesta dell'abbonato, di adottare le suddette «misure ragionevoli». Tale ultima posizione appare peraltro in piena coerenza con il suddetto paragrafo 2, il quale prevede che «*Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato […] a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali*».

Infine, con la terza questione, il giudice del rinvio ha richiesto se il regime di cd. *accountability* previsto dal GDPR (articoli 24 e 5, paragrafo 2) comporti per il titolare, ossia Proximus, l'implementazione di misure tecniche e organizzative adeguate per informare l'operatore di servizi telefonici che gli ha comunicato i dati personali del suo abbonato, nonché gli altri fornitori di elenchi telefonici ai quali egli stesso ha fornito

tali dati, della revoca del consenso da parte dell'interessato.

Anche in questo caso, la CGUE ritiene che la responsabilizzazione dei titolari del trattamento, sulla base del dettato del GDPR, richieda l'adozione di misure adeguate in tal senso.

La pronuncia della CGUE, a conclusione di un complesso iter processuale, ha l'importante compito di evidenziare i confini entro i quali si muove l'*accountability* del titolare del trattamento sulla base delle disposizioni del GDPR. Quest'ultimo, infatti, non è esonerato da responsabilità nei confronti degli interessati per il solo fatto di aver rimosso o cancellato i dati personali del reclamante che ne ha fatto espresso richiesta e che abbia revocato il consenso per tale trattamento, bensì è tenuto ad adottare misure ragionevoli per informare i motori di ricerca e gli altri titolari del trattamento che gli hanno fornito tali dati o che li hanno ricevuti, della volontà di tale soggetto. Ne deriva che, nel caso in cui diversi titolari del trattamento si basino sul consenso unico dell'interessato, è sufficiente che quest'ultimo si rivolga a uno qualsiasi di essi per avere riconosciuta la sua pretesa anche nei confronti degli altri.

CARMINE ANDREA TROVATO

https://curia.europa.eu/juris/document/document.jsf;jsessionid=B7421151106ADD2C73E29024470A42DE?text=&docid=267605&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=64279

10. Verso l'Interoperable Europe Act: la proposta della Commissione di regolamento europeo sull'interoperabilità nel settore pubblico del 18.11.2022.

È del 21 novembre 2022 la notizia diffusa a mezzo stampa che la Commissione europea ha elaborato una proposta di regolamento sulla '*Europa interoperabile*' per permettere alle amministrazioni nazionali di condividere dati e soluzioni informatiche innovative (come software open-source, linee guida, liste di controllo, quadri e strumenti informatici) nel settore pubblico. Si tratta della proposta COM(2022) 720 final del 18 novembre 2022, di un regolamento che stabilisce misure per un "alto livello di interoperabilità nel settore pubblico nell'Unione" c.d. *Interoperable Europe Act*.

Il regolamento istituirà una rete di amministrazioni per migliorare i servizi resi alla cittadinanza, stimolare l'innovazione digitale anche d'intesa col mondo imprenditoriale e contenere la spesa pubblica.

A ispirarla è il concetto di "interoperabilità" intesa come capacità delle amministrazioni di cooperare e far funzionare i servizi offerti al pubblico al di là delle frontiere, dei settori e dei confini organizzativi. Il quadro di cooperazione transfrontaliera così ideato dovrebbe contribuire a rimuovere gli oneri burocratici a carico delle imprese e dei cittadini che entrano in contatto con le amministrazioni, aumentandone la fiducia reciproca.

Nel dettaglio il progetto di legge istituirà un portale a libero accesso per condividere le soluzioni informatiche tra le amministrazioni dei singoli Stati membri; prevedendo al contempo metodologie comuni per valutare l'impatto dei sistemi informatici adoperati a livello nazionale anche con misure di valutazione periodica.

Il futuro quadro di cooperazione sarà guidato dal Comitato per l'Europa interoperabile composto da rappresentanti degli Stati membri dell'Unione, della Commissione, del Comitato delle Regioni e del Comitato economico e sociale europeo dotati di comprovata professionalità ed esperienza in campo digitale.

FILIPPO D'ANGELO

https://commission.europa.eu/system/files/2022-11/com2022720_0.pdf

11. I comunicati del Garante privacy italiano del 18.10.2022, del 21.10.2022 e del 12.11.2022 di avvio di istruttorie a carico di testate editoriali online per iniziative di cookie wall e monetizzazione di dati personali

Con tre comunicati emessi nell'arco di meno di un mese, il Garante italiano per la protezione dei dati personali (di seguito solo il "Garante") ha reso noto di aver sottoposto al suo esame e poi di aver avviato una serie di istruttorie in relazione a una serie di recenti iniziative di c.d. *paywall* e *cookie wall* poste in essere da una serie di soggetti tra cui diverse testate giornalistiche *online*.

Più precisamente, con un primo comunicato del 18 ottobre 2022, il Garante informava di aver cominciato ad esaminare - alla luce del quadro normativo attuale e al fine di valutare l'adozione di

eventuali provvedimenti di sua competenza - recenti iniziative di *paywall* e *cookie wall* poste in essere da una serie di soggetti (non nominati) rispondenti a diverse testate giornalistiche *online*, siti *web* e aziende operanti su Internet nel settore televisivo. Nel comunicato in questione si specificava che le iniziative sottoposte all'esame del Garante riguardavano la messa in campo di sistemi e filtri che condizionano l'accesso ai contenuti alla sottoscrizione di un abbonamento (c.d. *paywall*) o, in alternativa, al rilascio del consenso da parte degli utenti all'installazione di *cookie* e altri strumenti di tracciamento dei dati personali (c.d. *cookie wall*).

Con il secondo comunicato di tre giorni dopo (21 ottobre), il Garante, riferendosi alle medesime iniziative, informava di aver deciso di avviare una serie di istruttorie, a ciò premettendo il rilievo che "la normativa europea sulla protezione dei dati personali non esclude in linea di principio che il titolare di un sito subordini l'accesso ai contenuti, da parte degli utenti, al consenso prestato dai medesimi per finalità di profilazione (attraverso *cookie* o altri strumenti di tracciamento) o, in alternativa, al pagamento di una somma di denaro".

Infine, con il terzo comunicato del 12 novembre 2022, il Garante si riferiva soltanto alle testate giornalistiche *online* informando della prosecuzione delle istruttorie aventi ad oggetto le iniziative di condizionare l'accesso ai loro contenuti al consenso a trattamenti di profilazione (attraverso *cookie* o altri strumenti di tracciamento) o, in alternativa, al pagamento di una somma di denaro. Il Garante specificava che le istruttorie sono finalizzate a valutare la liceità di tali iniziative, di aver rivolto alle testate giornalistiche *online* una serie di richieste di informazioni e di voler condurre una serie di approfondimenti su specifici temi. In particolare, con il terzo comunicato, il Garante informava il pubblico di aver rivolto alle testate giornalistiche *online* una serie di domande volte ad accertare le modalità di funzionamento del predetto meccanismo di condizionamento, comprese le diverse tipologie di scelte a disposizione dell'utente, e ad accertare il rispetto della normativa in materia di protezione dei dati personali, in particolare con riguardo alla correttezza e alla trasparenza dei trattamenti e al requisito della libertà del consenso. Quanto agli approfondimenti, il Garante informava di voler esaminare le valutazioni di impatto eventualmente effettuate dai gruppi editoriali, come pure le analisi e i criteri adottati per la determinazione del prezzo dell'abbonamento alternativo al servizio disponibile mediante prestazione del consenso.

SALVATORE ORLANDO

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9822601

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9816536

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9815415

12. Il comunicato del 14.11.2022 del Garante privacy italiano di avvio di istruttorie per i sistemi di videosorveglianza dei Comuni di Lecce e Arezzo.

Il 14.11.2022, il Garante privacy ha emesso un comunicato stampa, rendendo noto l'avvio di due procedimenti istruttori nei confronti dei Comuni di Lecce ed Arezzo, entrambi prossimi all'impiego di sistemi di videosorveglianza intelligente.

Nello specifico, il Comune di Lecce ha annunciato l'imminente adozione di un sistema che prevede il ricorso a tecnologie di riconoscimento facciale.

Al riguardo, l'Autorità ha ricordato che il trattamento di dati personali da parte di soggetti pubblici mediante dispositivi video è lecito e consentito se necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (v. art. 6, lett. *e*) GDPR) e, nello specifico, se svolto a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica (cfr. artt. 1, co. 2 e 5, co. 1 d.lgs. 18 maggio 2018, n. 51 attuativo della direttiva 2016/680/UE, c.d. direttiva Law Enforcement).

Nondimeno, per i Comuni, l'impiego di impianti di videosorveglianza è consentito solo a condizione che venga stipulato un cosiddetto "patto per la sicurezza urbana tra Sindaco e Prefettura".

Inoltre, ai sensi dell'Allegato alla l. 3 dicembre 2021, n. 205, di conversione del c.d. Decreto Capienze, d.l. 8 ottobre 2021, n. 139, in assenza di una specifica legge in materia, e comunque fino al 31 dicembre 2023, sono sospesi in Italia l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici, a meno che il trattamento non sia effettuato dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali, previo parere favorevole del Garante privacy reso ai sensi dell'art. 24, co. 1, lett. *b*) del

richiamato d.lgs. n. 51/2018, ovvero dall'autorità giudiziaria nell'esercizio delle funzioni di indagine o di prevenzione e repressione dei reati.

La moratoria nasce dall'esigenza di disciplinare requisiti di ammissibilità, condizioni e garanzie relative al riconoscimento facciale, nel rispetto del principio di proporzionalità di cui all'art. 52 par. 1 della Carta dei diritti fondamentali dell'Unione Europea (CDFUE).

Il Comune di Lecce dovrà quindi fornire all'Autorità una descrizione dei sistemi adottati, le finalità e le basi giuridiche dei trattamenti, un elenco delle banche dati consultate dai dispositivi, nonché adottare e trasmettere la valutazione d'impatto sulla protezione dei dati che l'art. 35, par. 3, lett. *c*) GDPR prescrive in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il secondo procedimento ha interessato il Comune di Arezzo, che, secondo notizie di stampa, avrebbe intenzione di dar avvio, a partire dal 1° dicembre 2022, alla sperimentazione di "super-occhiali infrarossi". Tali dispositivi, in dotazione agli agenti della Polizia locale, sarebbero in grado di rilevare in tempo reale le infrazioni facenti capo al proprietario del veicolo tramite la lettura del numero di targa delle autovetture. Inoltre, attraverso il collegamento ad alcune banche dati nazionali, sarebbe possibile verificare la validità dei documenti del guidatore e acquisire alcune informazioni quali, ad esempio, la quantità dei punti residui sulla patente o prescrizioni come l'obbligo di indossare occhiali o lenti a contatto durante la guida.

L'Autorità ha prontamente ammonito il Comune di Arezzo di tenere debitamente in conto i rischi che l'uso di siffatti dispositivi possono comportare tanto sul versante della tutela dei dati personali quanto su quello dei diritti dei lavoratori. A preoccupare è soprattutto la circostanza che tali strumenti possano comportare, anche indirettamente, un controllo a distanza sulle attività del lavoratore, ammissibile solo alle condizioni e con le cautele prescritte dall'art. 4 dello Statuto dei lavoratori (l. 300/1970, come emendata *in parte qua* dall'art. 23 d.lgs. 14 settembre 2015, n. 151 e dall'art. 5, co. 2 del d.lgs. 24 settembre 2016, n. 185). A tal fine, il comma 3 della citata disposizione impone che sia fornita al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e reclama il rispetto della disciplina del Codice in materia di protezione dei dati personali.

Pertanto, il Comune di Arezzo dovrà fornire copia dell'informativa da rendere agli interessati, cioè a dire tanto ai cittadini proprietari dei veicoli, ai sensi dell'art. 13 GDPR, quanto al personale della forza pubblica. A ciò si accompagna l'obbligo di adozione della valutazione d'impatto sulla protezione dei dati di cui all'art. 35 GDPR.

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9823282

13. La sentenza Cassazione Sez. 2 Penale n. 44378/2022 del 26.10.2022 sulla qualificazione della moneta virtuale e delle Initial Coin Offerings (a proposito di un sequestro penale preventivo di wallet contenente bitcoin e di una fattispecie di reato di abusivismo finanziario ai sensi dell'art. 166 co. 1 TUF)

Con sentenza del 26 ottobre 2022 la Corte di Cassazione, Sez. II Penale, si è pronunciata sul ricorso presentato dal Pubblico Ministero di Brescia avverso la decisione del Tribunale di Brescia, in funzione di giudice del riesame, sull'ordinanza del GIP di Brescia che aveva rigettato la richiesta di sequestro preventivo di un *wallet* contenente 30 Bitcoin.

Il fatto.

Nel 2017 il Sig. S. M. lanciava una *Initial Coin Offering* (c.d. ICO) la quale prevedeva l'emissione di criptoattività denominate "LWF Coin" (di seguito anche i "**Coin**") a fronte dell'apporto di Bitcoin da parte degli "investitori". L'offerta di tali criptoattività era funzionale alla costituzione di una piattaforma di logistica multi-servizio che gli investitori avrebbero potuto utilizzare servendosi degli LWF Coin. Stando a quanto riportato dalla sentenza, i token offerti sembrerebbero riconducibili alla categoria degli "**utility token**" i quali consentono la fruizione di un bene o servizio fornito dall'emittente del token medesimo. Non si tratterebbe, dunque, di "**security token**" che, invece, sostanzialmente rappresentano la proprietà di un asset da cui dipende il valore del token medesimo. L'emissione delle criptoattività, nonché i diritti amministrativi e patrimoniali dei possessori degli LWF Coin era regolata da un *white paper* pubblicato proprio per l'offerta dei Coin.

Per quanto qui interessa, siccome l'offerta al pubblico di prodotti finanziari è soggetta ad una serie di obblighi, che la Procura riteneva non rispettati dal Sig. S. M., quest'ultimo veniva

indagato per il reato di abusivo esercizio di offerta al pubblico di prodotti finanziari di cui all'art. 166 D. Lgs. 58/1998 (c.d. TUF). Al fine di stabilire se sussistessero i reati in parola la Suprema Corte, dunque, si è interrogata sulla natura delle cripto-valute e, di riflesso, sulla qualificazione giuridica di un *Initial Coin Offering*.

La normativa di riferimento.

Ai fini della presente analisi, innanzitutto, occorre considerare l'art. 1 della dir. 2018/843/UE che definisce le valute virtuali come "*una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente*".

La normativa europea è stata recepita dal Legislatore italiano con il D. Lgs. 125/2019 che ha modificato l'art. 1 D. Lgs. 231/2007 il quale così definisce le valute virtuali: "*la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente*" (art. 1 let. qq) D. Lgs. 231/2007). Come rilevato anche dalla Suprema Corte, tale definizione aggiunge alla normativa europea la finalità di investimento quale scopo della valuta virtuale.

Nondimeno, il D. Lgs. 231/07 definisce pure:

1) i prestatori di servizi relativi all'utilizzo di valuta virtuale come la "*persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche online, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute*" (art. 1, let. ff) D. Lgs. 231/2007);

2) i prestatori di servizi di portafoglio digitale come "*ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*" (art. 1, let. ff bis) D. Lgs. n. 231/2007).

L'art. 17 bis, commi 8 bis e ter D. Lgs. 141/2010 impone ai suddetti prestatori di servizi di comunicare la loro operatività in Italia, nonché di iscriversi alla **sezione speciale del registro dei cambiavalute tenuto dall'Organismo Agenti e Mediatori** (su cui v. notizia n. 7 nel numero 1/2022 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf).

Ai fini della presente analisi, inoltre, sono particolarmente importanti l'art. 1, lett. u) e l'art. 1, co. 2 TUF i quali, rispettivamente, definiscono i prodotti finanziari, come "*gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria*", e gli strumenti finanziari, rinviando ad un allegato al TUF.

Nondimeno, l'art. 94 TUF assoggetta l'offerta al pubblico di prodotti finanziari a determinati adempimenti, tra cui la predisposizione del prospetto. La violazione di tali obblighi è un reato punito dall'art. 166 TUF.

I precedenti giurisprudenziali (e un cenno alla dottrina).

La Suprema Corte si è già espressa sul tema della qualificazione delle criptovalute.

In particolare, nelle sentenze n. 26807/2020 e n. 44337/2021 la Corte di Cassazione Penale ha equiparato le criptovalute ai prodotti finanziari (non agli strumenti finanziari), ritenendo applicabile la relativa disciplina, poiché tali criptoattività erano state offerte con modalità tali da essere equiparate ad un offerta al pubblico di prodotti finanziari ovvero da far sorgere l'aspettativa di un rendimento.

Nella sentenza n. 2736/2013, inoltre, la Corte di Cassazione Civile ha stabilito che la qualificazione di un asset come prodotto finanziario non può dipendere dalla motivazione (elemento soggettivo) di chi lo acquista, ossia la volontà di fare un investimento, ma dalla causa dell'operazione (elemento oggettivo).

Anche la giurisprudenza di merito si è espressa la riguardo.

In particolare, il Tribunale di Verona con una sentenza del 24 gennaio 2017, a cui si conforma anche la pronuncia in commento, ha stabilito che i caratteri di un "investimento finanziario" sono: i) un impiego di capitali; ii) un'aspettativa di rendimento; iii) la rischiosità dell'attività in cui si investe. Secondo il Tribunale di Verona le valute virtuali, acquistate su una piattaforma di scambio, presentano tutte le suddette caratteristiche e sono equiparabili agli "strumenti finanziari".

Per quanto qui interessa, va detto, sia pur brevemente, che la dottrina si è più volte espressa sulla qualificazione di un asset (nel nostro caso le criptovalute) come prodotto o strumento finanziario.

Ora, è noto che gli strumenti finanziari sono un numero chiuso giacché sono solo quelli indicati nella sezione C dell'Allegato I al TUF. È stato rilevato, tuttavia, che, alla luce della costante evoluzione del mondo della finanza, il confine tra prodotti e strumenti finanziari è labile. Ciò che li distingue, dunque, "*è la caratteristica della potenziale negoziabilità nel mercato dei capitali, condizione necessaria per …* [nds, gli strumenti] *ma non per …* [nds, i prodotti]".

Conclusioni. Il ragionamento della Corte.

Nel caso di specie la Cassazione, probabilmente animata dall'intenzione di tutelare gli investitori, ritiene che l'ICO degli LWF Coin rispetti tutti i requisiti elencati dalla pronuncia del Tribunale di Verona e pertanto "*la valuta virtuale deve essere considerata strumento di investimento perché consiste in un prodotto finanziario, per cui deve essere disciplinata con le norme in materia di intermediazione finanziaria".* Di conseguenza, l'*Initial Coin Offering* svolta dal Sig. S.M. sostanzialmente consisteva in un'offerta al pubblico di valute virtuali, ma senza predisporre un vero prospetto - tranne il menzionato *white paper* – e senza che l'offerente fosse iscritto alla sezione speciale del registro dei cambiavalute. Essa, dunque, è da ritenersi abusiva e integrante il reato ex art. 166 TUF.

Se l'intenzione di tutelare gli investitori che anima la Corte è apprezzabile, bisogna però rilevare l'imprecisione terminologica della sentenza in commento che parla di "*strumento di investimento"* il quale, però, non è una fattispecie esistente nel nostro ordinamento. Considerata la rapida evoluzione della normativa e della prassi in materia, tale imprecisione non aiuta.

In secondo luogo, la sentenza fonda l'equiparazione tra criptovalute e prodotti finanziari su un elemento soggettivo quale l'aspettativa di un rendimento, invece che su elementi oggettivi come la causa del negozio giuridico o la funzione del rapporto giuridico. La suddetta equiparazione, peraltro, contravviene alla suddetta pronuncia n. 2736/2013 senza motivare ed analizzare la causa negoziale dell'operazione e del white paper che accompagnava l'ICO.

Per di più, la Consob ha rilevato che i rendimenti dei token (peraltro qui si tratterebbe di utility e non security token) di per sé "*non sono chiaramente ricollegabili ai "rendimenti di natura finanziaria"*" (CONSOB, Le offerte iniziali e gli scambi di cripto-attività, 2019). L'equiparazione tra criptovalute e strumenti finanziari, dunque, non è scontata.

Infine, va detto che la pronuncia in commento non si concilia con le previsioni della proposta di **Regolamento sui mercati delle criptovalute** (c.d. MiCAR, acronimo che sta per Markets in Crypto-Assets Regulation: su cui v. notizia n. 3 nel numero 2/2022 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2022/08/Osservatorio-2-2022.pdf), che, da un lato, esclude un obbligo di prospetto per l'offerta di criptovalute e, dall'altro, non assoggetta quest'ultima alle norme sull'offerta a distanza di prodotti finanziari.

EMANUELE STABILE

https://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snpen&id=./20221122/snpen@s20@a2022@n44378@tS.clean.pdf

14. L'ordinanza Cassazione Sez. 1 Civile n. 34658/2022 del 24.11.2022 sul diritto all'oblio e l'ordine di rimozione c.d. globale (regime Codice privacy anteriore al GDPR)

Con l'ordinanza della Prima Sez. Civile n. 34658/2022 del 24.11.2022, i giudici di legittimità si sono pronunciati nuovamente sul diritto all'oblio (sulla sentenza della Cassazione n. 3952 del 8 febbraio 2022 sul diritto all'oblio e le copie *cache*, v. la notizia n. 12 nel numero 1/2022 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf), in particolare sotto il profilo dell'estensione territoriale degli ordini di rimozione o deindicizzazione. La Suprema Corte ha accolto il ricorso proposto dal Garante per la protezione dei dati personali (di seguito anche solo il "Garante") nei confronti di Google LLC (di seguito anche solo "Google"), affermando che, in tema di trattamento dei dati personali, la tutela spettante all'interessato, strettamente connessa ai diritti alla riservatezza e all'identità personale è preordinata a garantire la dignità personale dell'individuo, ai sensi dell'art. 3 Cost., comma 1 e dell'art. 2 Cost. Pertanto, il cosiddetto "diritto all'oblio", consente, in conformità al diritto dell'Unione Europea, alle autorità italiane di ordinare al gestore di un motore di ricerca di effettuare una deindicizzazione su tutte le versioni, anche extraeuropee, di tale motore, previo bilanciamento tra il diritto alla tutela della vita privata e alla protezione dei dati personali e il diritto alla libertà di informazione, da operarsi

secondo gli standard di protezione dell'ordinamento italiano.

La vicenda trae origine dall'ordine dato dal Garante a Google di rimuovere, anche dalle versioni extraeuropee del motore di ricerca, gli URL oggetto della richiesta di un interessato che, avendo interessi professionali al di fuori del territorio dell'Unione, chiedeva l'applicazione extraterritoriale della misura. Contestando proprio l'estensione globale del provvedimento, Google chiedeva l'annullamento dello stesso al Tribunale di Milano, che accoglieva il ricorso e riteneva applicabile *ratione temporis* alla fattispecie la Direttiva 95/46/CEE, attuata in Italia con il d.lgs. 196 del 2003 ("**Codice Privacy**"), in quanto all'epoca dei fatti non era ancora entrato in vigore il Regolamento UE 2016/679 ("**GDPR**"). Sulla base dell'applicazione della normativa precedente, il Tribunale meneghino rilevava la mancata previsione di una norma che legittimasse l'estensione extraterritoriale del provvedimento, censurando quest'ultimo anche sotto il profilo del bilanciamento tra diritto dell'interessato e libertà di informazione.

Avverso tale sentenza ha proposto ricorso per cassazione il Garante, sulla base di tre motivi.

Con il primo motivo di ricorso, il Garante ha eccepito la violazione e falsa applicazione delle norme del previgente Codice Privacy, laddove il Tribunale ha negato la possibilità di una applicazione extraterritoriale delle stesse, già ammessa dalla CGUE in casi recenti.

Con il secondo motivo di ricorso, il Garante contestava l'interpretazione secondo cui il bilanciamento di interessi, sotteso all'applicazione di una misura di deindicizzazione, doveva essere parametrato ai diversi ordinamenti esistenti nei Paesi extra UE ove il provvedimento avrebbe dovuto spiegare i suoi effetti.

In ultimo, con il terzo motivo, il Garante eccepiva la contraddittorietà della sentenza impugnata, laddove è stato ritenuto insufficiente il materiale probatorio a supporto di un interesse ad un provvedimento extraterritoriale.

È opportuno ricordare come la Suprema Corte aveva precedentemente affermato che il diritto all'oblio consiste *"nel non rimanere esposti senza limiti di tempo ad una rappresentazione non più attuale della propria persona con pregiudizio alla reputazione ed alla riservatezza"* (Cass. Civ. sez. I, n. 9147/20).

L'oggetto della pronuncia in commento concerne quella che parte della dottrina definisce come seconda accezione del diritto all'oblio, da ricondurre alla tutela dell'identità personale. In quest'ottica, il bene giuridico tutelato è più ampio rispetto al singolo dato personale, mirando a tutelare a tutto tondo la dignità della persona, sotto il profilo della sua identità. Ne discende la necessità di contestualizzare le informazioni, valutando l'impatto di queste ultime sull'individuo in relazione alla situazione nella quale egli si trova in quello specifico momento.

Nella medesima pronuncia, la Corte affronta il tema del difficile bilanciamento fra il diritto all'oblio e il diritto di cronaca/informazione, che rappresenta uno degli aspetti più delicati e problematici dell'attuazione di questa disposizione. A norma dell'art. 17, comma 3, lett. a) GDPR, l'esercizio della libertà di espressione e di informazione costituisce una delle eccezioni che consentono di escludere l'esercizio del diritto all'oblio, rendendo necessaria un'analisi svolta caso per caso e volta a valutare la prevalenza dell'uno o dell'altro nelle circostanze concrete (es. l'interessato è un personaggio pubblico, i fatti riportati sono inaccurati etc.). Limitare la portata del diritto all'oblio alla sola cancellazione dei dati, vorrebbe dire snaturare ingiustamente la disposizione. Questa, infatti, anche alla luce dell'interpretazione datane dalla giurisprudenza, ammette, fra le misure che ne permettono la piena attuazione, la deindicizzazione, l'anonimizzazione dei dati e la loro esatta contestualizzazione.

Ciò considerato, relativamente alle questioni rilevanti per la definizione del caso in oggetto, la Cassazione ha individuato tre precedenti della CGUE (C-131/12, C-507/20 e C-18/08) che, pur giungendo a conclusioni differenti tra loro, permettono di stabilire chiaramente come il diritto dell'Unione non imponga che la deindicizzazione accolta verta su tutte le versioni del motore di ricerca, ma neppure lo vieta. Pertanto, spetta all'autorità di controllo o all'autorità giudiziaria di uno Stato membro effettuare il bilanciamento tra, da un lato, il diritto della persona interessata alla tutela della sua vita privata e alla protezione dei suoi dati personali e, dall'altro, il diritto alla libertà d'informazione. Al termine della valutazione suesposta, sarà discrezione dell'autorità competente richiedere al motore di ricerca una deindicizzazione su tutte le versioni dello stesso o meno.

Alla luce di quanto sopra e riconoscendo il rango costituzionale assunto dal diritto alla protezione dei dati personali, tra cui rientra la riservatezza garantita dal diritto all'oblio, la Corte di Cassazione ha concluso per l'accoglimento del ricorso presentato dal Garante, ammettendo la portata extraterritoriale del provvedimento di deindicizzazione, restando impregiudicata sia la sovranità dello Stato straniero destinatario della misura sia la possibilità per quest'ultimo di non

riconoscere il provvedimento o la decisione giurisdizionale che lo ha ritenuto legittimo.

EMANUELA BURGIO

https://web.uniroma1.it/deap/sites/default/files/allegati/cass34658_22.pdf

15. La sentenza Tar Campania, sede di Napoli, Sez. III, n. 7003 del 14 novembre 2022 sull'uso di sistemi algoritmici nei procedimenti amministrativi

A proposito dell'uso di sistemi algoritmici nell'attività amministrativa (su cui v. in questa Rubrica le notizie n. 7 nel numero 4/2021 sulla sentenza del Tar Lazio n. 7589 del 24 giugno 2021 a proposito di procedure di mobilità nella pubblica amministrazione: http://www.personaemercato.it/wp-content/uploads/2021/12/Osservatorio-1.pdf; e la notizia n. 13 nel numero 1/2022 a proposito delle *Model Rules* elaborate dallo *European Law Institute* sulla valutazione di impatto delle decisioni algoritmiche nella pubblica amministrazione: http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf) si segnala una interessante sentenza del 14 novembre 2022 del TAR Campania – sede di Napoli, Sez. III, n. 7003 sull'uso di sistemi algoritmici nei procedimenti amministrativi per erogare i fondi agricoli gestiti dall'Agenzia per le Erogazioni in Agricoltura (AGEA) per conto della Commissione europea.

Questi i passaggi più significativi della pronuncia.

Anzitutto il giudice napoletano ha precisato che la decisione algoritmica si rivela di particolare utilità nei procedimenti amministrativi in cui "occorre gestire un numero notevole di istanze, per la cui elaborazione l'impiego dello strumento algoritmico consente una maggiore velocità, efficienza ed in astratto maggiore imparzialità".

Secondo il Tribunale campano, il pregio del mezzo informatico è infatti la "invariabilità dell'esito: i 'termini' dell'algoritmo, combinati nel modo assunto dallo stesso, portano sempre e invariabilmente allo stesso risultato" con una "decisione spogliata da ogni margine di soggettività".

Tuttavia, rileva il Giudicante, la procedura informatizzata deve essere controbilanciata dal "controllo umano del procedimento, in funzione di garanzia (cd. *human in the loop*), in modo che il funzionario possa in qualsiasi momento intervenire per compiere interlocuzioni con il privato, per verificare a monte l'esattezza dei dati da elaborare, mantenendo il costante controllo del procedimento".

L'uso dell'algoritmo, in altre parole, secondo questa sentenza, sta in "funzione integrativa e servente della decisione umana" e "non può mai comportare un abbassamento del livello delle tutele garantite dalla legge sul procedimento amministrativo" (in particolare la trasparenza del processo decisionale e l'obbligo di motivazione del provvedimento finale).

Significativo anche il passaggio nel quale il TAR campano dichiara che l'amministrazione procedente deve dedicare particolare attenzione ai termini di "costruzione dell'algoritmo"; al modo in cui i "para-metri dell'algoritmo vengono scelti (operazione di per sé soggettiva), e come si combinano tra loro"; alla "conoscibilità della costruzione dell'algoritmo, anche, eventualmente, in funzione del sindacato sull'atto adottato sulla base dello stesso".

Quest'ultima, in particolare, rileva il Tribunale amministrativo, "deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti".

Tanto, in conclusione, impone all'amministrazione di rendere comprensibile a chiunque il linguaggio informatico utilizzato dai creatori dell'algoritmo attraverso documenti esplicativi; e di revisionare, ove occorra, il sistema algoritmico attraverso "costanti test, aggiornamenti e modalità di perfezionamento".

FILIPPO D'ANGELO

https://www.giustizia-amministrativa.it/

16. L'ordinanza del Tribunale di Roma del 20.7.2022 sui Non-Fungible Tokens (NFT): il caso della Juventus

Il Tribunale di Roma (Sez. XVII Imprese Civ.), con ordinanza cautelare del 20 luglio 2022 ha disposto un ordine di inibitoria dalla creazione e commercializzazione di *Non-Fungible Tokens* (**NFT**) in violazione di marchi registrati, oltre al ritiro dal commercio e la rimozione degli stessi NFT da ogni sito Internet.

Si tratta del primo provvedimento cautelare noto di una corte europea che stabilisce che i NFT

che riproducono senza autorizzazione i marchi di terzi costituiscono una violazione, concedendo la relativa ingiunzione al titolare dei diritti. Ad oggi, a livello internazionale, sono conosciute solo decisioni similari emesse a Singapore e in Turchia.

Nonostante non sia ancora chiaro né l'inquadramento giuridico dei NFT né la loro definizione, l'Ufficio dell'Unione europea per la proprietà intellettuale (EUIPO) suggerisce di considerarli come "*certificati digitali unici, registrati in una blockchain, utilizzati come mezzo per registrare la proprietà di un oggetto, come un'opera d'arte digitale o un oggetto da collezione*" (EUIPO Draft Guidelines 2023 edition, su https://euipo.europa.eu/ohimportal/nl/draft-guidelines-2023).

Nel caso di specie, la società Blockeras s.r.l. ("**Blockeras**") aveva mintato e commercializzato alcuni NFT associati a immagini di un noto calciatore con la maglia della Juventus Football Club S.p.A. ("**Juventus**"), senza aver ottenuto il consenso dalla società di calcio.

La Juventus conveniva Blockeras avanti alla Sezione Specializzata del Tribunale di Roma lamentando la violazione sia del marchio figurativo, costituito dalla maglia a strisce verticali bianche e nere con due stelle sul petto, sia dei propri marchi denominativi JUVENTUS e JUVE.

La Blockeras si era opposta alla concessione delle misure inibitorie alla luce dell'autorizzazione all'uso dell'immagine ottenuta dal calciatore, evidenziando sia che i marchi della Juventus non risultavano registrati per prodotti virtuali sia l'assenza del "*periculum in mora*".

Il 20 luglio 2022, il Tribunale ha accolto le domande della ricorrente, ritenendo che Blockeras avesse adottato comportamenti integranti le fattispecie di concorrenza sleale (che potrebbe contribuire alla "volgarizzazione del marchio, provocando un danno con obiettive difficoltà di quantificazione") e appropriazione dei pregi connessi ai marchi utilizzati, che costituiscono un pericolo di danno per la Juventus.

Il Tribunale ha confermato la notorietà dei marchi e ha respinto l'affermazione di Blockeras secondo cui i diritti di marchio della Juventus erano limitati a una classe di prodotti diversa da quella dei prodotti digitali creati e venduti dalla società, infatti, i particolari contenuti digitali in questione devono essere considerati inclusi nella Classe 9 della Classificazione di Nizza ("inerenti anche a pubblicazioni elettroniche scaricabili"), oggetto di registrazione da parte della Juventus**:** come da interpretazione di EUIPO secondo cui la classe 9 è deputata alla registrazione di marchi utilizzati per caratterizzare determinate categorie di "beni digitali".

Il Tribunale ha rilevato come l'autorizzazione concessa dal giocatore all'utilizzo della propria immagine non escludesse la necessità di chiedere l'autorizzazione anche all'uso dei marchi registrati della squadra di cui erano riprodotte le maglie e la denominazione, in quanto si trattava di beni destinati alla vendita commerciale, in relazione alle quali anche la fama delle diverse squadre in cui il calciatore ha giocato contribuiscono a dare valore all'immagine digitale da acquistare; come disposto dall'art. 97 della Legge sul Diritto d'Autore, l'uso consentito del diritto all'immagine di una persona non si estende anche all'uso dei marchi rappresentati nella medesima immagine.

In merito al "periculum in mora", il Tribunale ha confermato la sussistenza del requisito in esame rilevando un "attuale possibilità di rivendita, nel mercato secondario, delle Cards già acquistate dagli utenti" anche considerando che i NFT, essendo già stati acquistati, non si trovavano più nella disponibilità di Blockeras.

Il Tribunale ha disposto pertanto un ordine "nei confronti della società resistente di ritirare dal commercio e rimuovere da ogni sito internet e/o da ogni pagina di sito internet direttamente e/o indirettamente controllati dalla stessa su cui tali prodotti sono offerti in vendita e/o pubblicizzati, i NFT ed i contenuti digitali ad essi associati o prodotti in genere oggetto di inibitoria".

L'ordinanza cautelare, oltre a disporre l'inibitoria, è accompagnata da una penale per ogni giorno di ritardo o violazione (dalla "ulteriore produzione, commercializzazione, promozione e offerta in vendita, diretta e/o indiretta, in qualsiasi modo e forma, dei NFT e dei contenuti digitali di cui in narrativa, nonché di ogni altro NFT, contenuto digitale o prodotto in genere recante la fotografia di cui in narrativa, anche modificata, e/o i marchi di Juventus di cui in narrativa, nonché l'uso di detti marchi in qualsiasi forma e modalità"). Interessante evidenziare come nell'ingiunzione il Tribunale distingua tra i NFT e le immagini digitali associate agli stessi NFT ("gli NFT e i contenuti digitali ad essi associati") quasi a suggerire che i NFT abbiano autonomia giuridica rispetto ai contenuti ad essi associati (e.g. fotografie, opere musicali, etc.).

La decisione in oggetto conferma, in primo luogo, la possibilità di ottenere la tutela del marchio anche per quanto riguarda gli usi non autorizzati in contesti virtuali, e, in secondo luogo, l'opportunità di estendere la registrazione del marchio alle classi della Classificazione di Nizza che consentono l'uso del marchio stesso nella sfera digitale.

In conclusione, appare evidente dal provvedimento in oggetto come chiunque abbia intenzione di creare NFT dovrebbe prima procedere a una accurata *due diligence* che verifichi l'eventuale esistenza di diritti di proprietà intellettuale e di diritti della persona gravanti sui contenuti da associarvi.

FRANCESCO GROSSI

https://web.uniroma1.it/deap/sites/default/files/allegati/Trib_Roma_2022_Juve_NFT.pdf

17. L'order del 7.11.2022 della District Court of New Hampshire (USA) sulla qualificazione di un utility token come security.

Il 7 novembre del 2022 la District Court del New Hampshire, negli Stati Uniti, si è espressa sul caso *Securities Exchange Commission v. LBRY, Inc.* in tema di *utility token* e della relativa loro qualificazione giuridica.

Nel caso di specie, la Securities Exchange Commission ("**SEC**") richiedeva un provvedimento cautelare (*summary judgement*) in merito alle attività svolte dalla società del New Hampshire, la LBRY, Inc. ("**LBRY**"), che emette e vende specifici *blockchain token*, dal nome "*LBRY Credits*" o "*LBC*" la cui natura giuridica, e specificamente la loro qualificazione come *unregistered securities* ai sensi della normativa statunitense applicabile (Sezione 5 del *Securities Act* del 1933), era affermata dalla SEC e negata da LBRY.

LBRY, fondata nel 2015, è una piattaforma digitale dotata di tecnologia blockchain che offre servizi di file sharing e dispone di una rete decentralizzata per i pagamenti online. Come illustrato nel provvedimento, gli LBC assolvono una serie di funzioni all'interno della LBRY Blockchain.

Nel caso di specie, la Corte ha voluto applicare il c.d. *Howey Test*, criterio elaborato nella storica sentenza *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946) per accertare la natura dell'operazione economica in analisi e verificare se essa possa qualificarsi come un contratto di investimento finanziario. A tal riguardo, la Corte, alla luce del suddetto test valutativo, ha ritenuto che le cripto-attività venissero offerte al pubblico e vendute in contrasto con la normativa federale in materia di *securities* in quanto l'operazione è da considerarsi come un contratto di investimento.

In relazione a questo ultimo aspetto, la Corte ha ricordato che il c.d. *Howey Test* si basi su tre principali requisiti: a) la presenza di un investimento economico e di capitale; b) la circostanza che il denaro è investito in una attività imprenditoriale specifica; c) la concreta aspettativa di un profitto rispetto al capitale investito.

Nel caso qui in analisi, la Corte ha sottolineato come soltanto l'ultimo requisito risultasse di maggiore complessità interpretativa, mentre i primi due criteri di valutazione erano da considerarsi pienamente sussistenti. A tal proposito, nella *opinion* della Corte, si è cercato di approfondire gli aspetti comunicativi connessi all'offerta di simili cripto-attività, per verificare la presenza di una legittima aspettativa in capo all'acquirente di un potenziale profitto in relazione al capitale inizialmente investito.

La Corte ha rilevato che LBRY avesse pubblicato numerose dichiarazioni che hanno portato i potenziali investitori di cripto-attività ad aspettarsi ragionevolmente che l'*utility token* così acquistato sarebbe cresciuto di valore sotto il controllo e la supervisione della società. In particolare, si mette in risalto come in alcune specifiche comunicazioni analizzate e illustrate dalla Corte nella pronuncia a titolo esemplificativo (un post all'interno del blog connesso alla piattaforma, una e-mail, una intervista sulle attività della società ed un post pubblicato su Reddit dal community manager della piattaforma) emergesse chiaramente l'intento di LBRY di ingenerare nella potenziale clientela la speranza di notevoli profitti derivanti dall'acquisto di questi particolari *utility token.* Per queste ragioni, è stato ritenuto soddisfatto anche il terzo requisito del c.d. *Howey Test* e, quindi, è stata qualificata l'intera operazione come un contratto di investimento.

In merito, inoltre, alle argomentazioni sostenute in giudizio da LBRY, la Corte ha respinto ogni posizione difensiva della società, rimarcando l'essenza effettiva delle operazioni economiche analizzate e la natura di investimento finanziario dei contratti sottesi.

La società, dal canto suo, aveva messo in risalto la natura di utilità del *token* acquistato e del consistente numero di acquirenti che aveva sottoscritto simili operazioni al fine di utilizzare le cripto-attività nell'ambito della sola piattaforma LBRY.

Sul punto, la Corte, però, ha espressamente sottolineato come risulti necessario analizzare la natura concreta del contratto in esame e che la commistione tra funzione consumeristica di utilità e funzione finanziaria di investimento non escluda la

possibilità di qualificare queste operazioni come contratti di investimento, alla luce dei precedenti applicabili al caso di specie e sulla base del c.d. *Howey Test.*

Dunque, la District Court del New Hampshire ha ritenuto *prima facie* che LBRY abbia immesso sul mercato prodotti che violano le regole vincolanti in materia di vendita di *securities*, celando la vera natura dei contratti sottoscritti dai singoli investitori.

In conclusione, il caso qui analizzato acuisce gli interrogativi circa la corretta applicazione della disciplina legale di riferimento in relazione a particolari tipologie di cripto-attività che, al di là delle funzioni consumeristiche o di utilità, presentano profili di rendimento finanziario o prospettive di profitto per gli investitori.

ENZO MARIA INCUTTI

https://www.crypto-law.us/wp-content/uploads/2022/11/Court-Decision-LBRY.pdf

18. L'Assurance of voluntary compliance tra Google e lo Stato della Pennsylvania (USA) del 14.12.2022 sui dati di localizzazione

Con "*effective date*" fissata al 14.12.2022, tra l'*Attorney General* del *First Judicial District* dello Stato della Pennsylvania Josh Shapiro (d'ora in poi "***Attorney General***") e Google LLC (d'ora in poi "**Google**") è intercorsa una c.d. *Assurance of voluntary compliance* (d'ora in poi "***Assurance***"), in base all'*Unfair Trade Practices and Consumer Protection Law*, 73 P.S. § 201-1, et seq.; 201-5 (d'ora in poi "***Consumer Protection Law***"). Analoghi accordi sono stati assunti nello stesso periodo tra Google e altri *Attorneys General* di numerosi altri Stati della Federazione.

L'*Assurance* è stata conclusa all'esito di un'istruttoria avviata dall'*Attorney General* in merito a talune pratiche occorse nel periodo dal 2014 al 2019, consistenti in false rappresentazioni e omissioni di informazioni, da parte di Google, relative alla raccolta, all'uso e alla conservazione di taluni tipi di dati riguardanti la posizione fisica di uno specifico utente o di uno o più dispositivi associati all'account di questi (d'ora in poi, "dati di localizzazione"). Le suddette condotte hanno riguardato, più in dettaglio, due impostazioni accessorie all'account che gli utenti di Google debbono creare per usufruire dei prodotti e servizi digitali forniti da tale società, la *Location History* e la *Web&App Activity*. La prima, quando attiva, raccoglie e conserva automaticamente nei server di Google dati di localizzazione dell'utente; la seconda, invece, registra anche tali tipi di dati, ogni qual volta l'utente interagisca con prodotti o servizi di Google (come YouTube o Google Search).

Google raccoglie i dati di localizzazione attraverso le ricordate impostazioni e li monetizza in un duplice modo: in primo luogo, ricavandone delle inferenze (ad es. dei profili), sulla cui base vengono personalizzati gli annunci pubblicitari mostrati a ciascun utente; in secondo luogo, ottenendone uno "*store convertion index*", un indice che misura il numero degli utenti i quali si recano presso una data attività commerciale (un "negozio fisico", come si direbbe in gergo), dopo aver ricevuto le relative comunicazioni pubblicitarie. La capacità di Google di "tracciare" gli spostamenti degli utenti, ne accresce il potere negoziale nei confronti delle controparti (gli "*advertisers*") con cui Google stessa stipula accordi nel mercato delle comunicazioni commerciali.

Secondo *l'Attorney General*, Google è incorsa in numerose violazioni della Consumer Protection Law, di seguito elencate:

1) *Location History* è preimpostata da Google come disabilitata ed attivabile soltanto per scelta dell'utente. Una prima pratica ingannevole tenuta da Google è consistita nell'aver dato ad intendere ai propri utenti che *Location History* costituiva l'unica impostazione deputata alla raccolta dei dati di localizzazione e che, una volta attivata, gli utenti avrebbero potuto in ogni momento decidere in senso contrario, nel qual caso i dati di localizzazione non sarebbero più stati conservati sui server della società.

Google ha omesso di informare gli utenti che, viceversa, anche una volta esclusa tale impostazione, i dati in questione potevano essere raccolti e conservati in altri modi, tra essi, attraverso *Web&App Activity* (che, ad esempio, registra e conserva il dato relativo al luogo in cui un utente compie una ricerca usando Google Search, alla località digitata su Google Maps per ottenere indicazioni stradali, etc.). *Web&App Activity* era preimpostata da Google come attiva, a meno che l'utente non si fosse adoperato per "disabilitarla". Fino al 2018, secondo le allegazioni dell'*Attorney General*, Google non ha reso nota agli utenti l'esistenza di tale ultima impostazione al momento della creazione dell'account e, soprattutto, non ha informato che anche tramite essa la società procedeva alla raccolta e immagazzinamento dei dati di localizzazione. Gli utenti venivano informati dell'esistenza di *Web&App Activity* soltanto al momento di accedere ad una separata pagina online,

dove pure, tuttavia, *Location History* veniva indicata come unico mezzo capace di raccogliere e conservare tali dati. Dopo tale data, Google ha bensì cominciato a fare menzione di *Web&App Activity* al momento della creazione dell'account, senza però svelarne la reale funzionalità (informazione, questa, acquisibile soltanto accedendo ad una apposita pagina web per mezzo di un link). Google ha dunque fuorviato i propri utenti non fornendo la ricordata informazione e dando ad intendere che questa forma di trattamento venisse svolta soltanto per mezzo di *Location History*. Inoltre, sempre Google ha falsamente suscitato negli utenti l'affidamento circa la capacità di controllare il trattamento dei dati di localizzazione attraverso l'impostazione del proprio account (con dichiarazioni del seguente tenore "Tu puoi sempre controllare come noi raccogliamo e usiamo questi dati ... Puoi sempre rettificare le tue impostazioni in un secondo momento o revocare il tuo consenso ...").

2) Non soltanto. Almeno fino a metà 2018, Google ha omesso di rivelare che procedeva al trattamento dei dati di localizzazione anche di utenti receduti dall'account ("*signed-out*"), quando utilizzano prodotti o servizi della società, e ciò per mezzo di un "identificativo univoco pseudonomizzato". Pertanto, Google non ha chiarito che un simile trattamento non cessava né quando l'utente faceva ricorso alle ricordate impostazioni, né con il recesso dall'account.
3) Google ha, infine, posto in essere una ulteriore pratica ingannevole, riguardante un altro tipo di impostazione, *Ads Personalization*, che consente agli utenti di revocare il consenso (implicitamente concesso al momento di creare l'account) a ricevere comunicazioni commerciali personalizzate in base alla loro posizione fisica. Google ha dichiarato che soltanto grazie a tale impostazione fosse in grado di inviare pubblicità personalizzata, mentre, in realtà, la società poteva ottenere altrimenti, per questa stessa finalità, dati di localizzazione, anche nel caso in cui la impostazione in parola fosse disattivata. Google ha dunque ingenerato negli utenti l'affidamento di essere in grado di controllare raccolta ed uso dei propri dati (la c.d. illusione di controllo) per fini di pubblicità personalizzata.

L'Assurance, oltre a prevedere una cospicua sanzione pecuniaria ed una serie di doveri di documentazione e di *reporting* periodico, contempla ordini diversi di "impegni" cui Google deve attenersi per un periodo di cinque anni (qui indicati riportando il numero dei relativi capoversi di cui l'Assurance consta).

La parte più rilevante di impegni riguarda le informazioni da fornirsi agli utenti circa il trattamento dei dati di localizzazione, nonché la possibilità per gli utenti di esercitare un controllo su simili dati.

In merito, è innanzitutto prescritto che Google comunichi, con uno specifico strumento di *legal design* (la "*pop-up notification*"), che *Location History* e *Web&App Activity* consentono di raccogliere dati di localizzazione; e che istruisca gli utenti sulle modalità per disattivare tali impostazioni, per stabilire limiti alla conservazione dei suddetti dati e per cancellarli.

E, inoltre, ivi previsto - sia rispetto agli account attivi, sia in relazione a quelli per cui è stato esercitato il recesso - che:

- siano fornite, attraverso una *webpage* dedicata, informazioni sulla raccolta e conservazione dei dati di localizzazione, con indicazione delle relative finalità, precisando se tra queste ultime rientrino finalità di profilazione e pubblicità personalizzata;

- gli utenti siano resi edotti della loro reale possibilità *i)* di limitare la raccolta e conservazione di tali dati, anche una volta che le suddette impostazioni siano state disabilitate; *ii)* di impedire l'uso da parte di Google dei dati di localizzazione per finalità di pubblicità personalizzata;

- sia chiaramente indicato agli utenti per quanto tempo Google immagazzina tali tipi di dati e, in caso affermativo, se allo spirare di tale periodo tali dati vengano cancellati da Google automaticamente o dietro richiesta degli utenti ovvero se sia prevista un'apposita funzionalità con cui l'utente possa procedere alla diretta cancellazione degli stessi;

- siano fornite indicazioni sulle tecniche di anonimizzazione, pseudonimizzazione, etc., adottate da Google e sulle finalità per le quali i dati vengono usati anche una volta sottoposti a tali tecniche.

Tutte le suddette informazioni debbono essere fornite in modo *clear and conspicuous*, vale a dire in modo tale che possano essere facilmente notate e comprese dall'utente, tenuto conto di una serie di dettagliate prescrizioni di legal design impartite dallo stesso *Attorney General* o individuate tramite rimando ai pertinenti standard tecnici (1, d).

Sono poi introdotte prescrizioni anche con riguardo al c.d. *Account Creation Flaw*, vale a dire alla *user interface* o al processo grazie ai quali

viene creato un account: all'atto della creazione di quest'ultimo, Google, non solo deve informare se raccoglie e conserva i suddetti dati, ma deve anche adottare certe modalità di interazione con gli utenti, atte a consigliare a questi ultimi di disattivare le impostazioni che siano attive *by default*.

Analoga finalità rivestono le prescrizioni con cui gli utenti vanno avvertiti del fatto che tali dati sono salvati e usati da Google solo se l'utente lo consente e che il controllo dei dati può essere esercitato dall'utente stesso attraverso una consapevole gestione delle impostazioni del proprio *account*.

Un ultimo ordine di prescrizioni, l'unico di natura non procedurale, concerne: i) il divieto per Google di condividere i dati di localizzazione con terze parti, in assenza di un consenso esplicito e formale dell'utente; ii) l'obbligo di cancellare automaticamente i dati di localizzazione conservati in *Web&App Activity* entro trenta giorni dalla loro raccolta; infine, iii) l'obbligo di cancellare i dati conservati in *Location History* e concernenti i c.d. Utenti Inattivi (vale a dire quelli i cui dati di localizzazione siano stati registrati un'ultima volta da più di tre anni) entro sei mesi da quando questi ultimi vengano di ciò avvertiti da Google con apposita comunicazione e in assenza di loro opposizione.

https://www.attorneygeneral.gov/taking-action/attorney-general-josh-shapiro-announces-391-million-settlement-with-google-over-location-tracking-practices/

ROBERTA MONTINARO

19. Le due sentenze "gemelle diverse" del Tar Lazio, sede di Roma, Sez. I del 18.11.2022 nei casi riguardanti Apple (sentenza n.15317) e Google (sentenza n.15326) in materia di pratiche commerciali sleali e patrimonializzazione dei dati personali

Con due sentenze decise in pari data (12.10.2022) e pubblicate in pari data (18.11.2022), il TAR Lazio, Roma, Sezione Prima, si è pronunciato, con esiti opposti, sulle impugnative proposte da Apple Distribution International Limited ("**Apple**") e Google Ireland Limited ("**Google**") avverso provvedimenti emessi nei loro confronti dall'Autorità Garante della Concorrenza e del Mercato ("**AGCM**" o l' "**Autorità**"). Si tratta di condotte e procedimenti distinti sotto ogni rispetto, che si riassumono qui di seguito in un'unica notizia soltanto perché le due pronunce riguardano la stessa normativa e sono state emanate in pari data dallo stesso Tribunale.

***

Con **sentenza n. 15317 del 18.11.2022**, il TAR Lazio, Roma, sez. I, in accoglimento del ricorso di Apple, ha annullato il provvedimento del 9.11.2021 (caso PS11150 - ICLOUD) con cui l'AGCM aveva comminato alla società del gruppo di Cupertino una sanzione di 10 milioni di euro complessivi, per due pratiche commerciali sleali limitative della libertà di scelta del consumatore medio.

La prima pratica (Condotta A), ritenuta scorretta, riguardava l'omessa informativa circa la raccolta e l'utilizzo dei dati personali degli utenti per finalità commerciali, sia durante la creazione dell'ID Apple (ossia l'identificativo che consente il riconoscimento dell'utente su più dispositivi, anche per l'accesso ai servizi iCloud) sia in fase di accesso agli Store (App Store, Libri e iTunes, dedicati rispettivamente ad app, libri e audiolibri e alla musica). La seconda pratica (Condotta B), ritenuta aggressiva, consisteva nella pre-impostazione del consenso degli utenti per acquisire i loro dati per le citate finalità commerciali, sia in fase di configurazione dell'Apple ID sia nelle pagine di accesso a ciascuno degli Store.

Dei dieci motivi di ricorso sollevati da Apple, il TAR ne ha rigettati tre di carattere procedurale, ne ha accolti cinque, incentrati sugli aspetti sostanziali relativi all'idoneità decettiva delle due pratiche, mentre due sono i motivi di ricorso rimasti assorbiti, e dunque non accolti e non rigettati.

Omettendo l'esposizione dei motivi di carattere procedurale, riassumiamo qui di seguito i motivi di carattere sostanziale.

Con i cinque motivi oggetto di accoglimento Apple aveva contestato: (1) il travisamento fattuale in cui era incorsa l'Autorità ritenendo che la configurazione dell'ID Apple implicasse la raccolta e il trattamento di dati personali degli utenti per finalità commerciali; (2) che la personalizzazione degli Store non dà luogo a cessione dei dati a terzi, né a sfruttamento economico dei dati, basandosi su un numero molto limitato di dati, ed essendo tali solo quelli strettamente necessari per fornire servizi personalizzati; (3) che il comportamento del consumatore medio negli Store non subisce alterazioni in virtù della personalizzazione, giacché, a differenza del caso in cui i servizi siano pubblicizzati come "gratuiti" (ad esempio, servizi di social media o di messaggistica istantanea), gli Store sono negozi digitali per la vendita di contenuti e, finché il consumatore non sceglie consapevolmente di effettuare un acquisto Apple non realizza alcun fatturato; (4) che l'informativa

che precede l'accesso agli Store è completa, poiché strutturata in modo tale da rendere gli utenti edotti che i loro dati di acquisto e ricerca possono essere utilizzati per la personalizzazione degli stessi Store; da ciò discende la liceità della Condotta A; (5) che il sistema opt-out di per sé non implica un indebito condizionamento dell'utente tale da porlo in una condizione coartata che ne pregiudica gli interessi; da ciò discende la liceità della Condotta B.

Analizzando i cinque motivi in questione congiuntamente, il TAR ha in primo luogo rilevato la differenza tra il caso in esame e le pratiche sanzionate dall'AGCM nei casi Facebook (Cons. Stato, sez. VI, 29 marzo 2021, n. 2631 - su cui v. la notizia n. 8 nel numero 2/2021 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio-1.pdf) e WhatsApp, avuto riguardo alla natura gratuita soltanto apparente del social network e della messaggistica istantanea con cui venivano promossi quei servizi per attrarre utenti, alla mole e alla natura dei dati acquisiti e trattati, all'assenza in quei contesti di un rapporto di stretta funzionalità tra servizio offerto (social network e messaggistica istantanea) e dati raccolti, nonché, in ultimo, allo sfruttamento economico "diretto" di tali dati mediante vendita/trasferimento a terzi.

Secondo il TAR, dalle evidenze raccolte in giudizio, emerge che il trattamento di dati a fini di personalizzazione delle email di marketing non avviene in seguito alla mera creazione di un ID Apple ma in seguito all'accesso degli utenti a ciascuno Store. Il TAR osserva inoltre che nel caso di specie manca anche il presupposto dell'uso diretto del dato fornito dall'utente, senza che questi ne sia a conoscenza, in quanto, da un lato, Apple fornisce agli utenti un'informativa di primo livello completa sulla "personalizzazione" degli Store, prima dell'accesso a tali spazi digitali; dall'altro, tale personalizzazione non comporta uno sfruttamento immediato e diretto delle informazioni raccolte: "*Apple genererà un profitto solo nel caso in cui gli utenti effettuino un successivo acquisto ovvero attraverso la vendita di pubblicità tramite la funzione "Search ads", che riguarda le app presenti nello store*".

Il TAR critica, inoltre, l'assunto dell'Autorità secondo cui i termini adoperati da Apple nell'informativa di primo livello, quale "personalizzazione", "consigli", "raccomandazioni", sarebbero ingannevoli, in quanto non idonei a far comprendere al consumatore la finalità commerciale della profilazione e che la personalizzazione dei dati forniti costituirebbe il mezzo e non il fine della "piattaforma". Tuttavia, osserva il TAR, "*l'Autorità non tiene conto di una circostanza di decisiva importanza, vale a dire che la piattaforma in questione è costituita da uno "store" - e quindi da un negozio virtuale - il cui accesso intrinsecamente presuppone la consapevolezza da parte dell'utente della natura commerciale delle transazioni che al suo interno possono essere eseguite*".

Dunque, benché sia ragionevole ipotizzare che la profilazione degli utenti possa consentire ad Apple di rendere più attrattivi gli Store, in ultima analisi, per accrescere il proprio fatturato, la condotta contestata secondo il TAR non può ritenersi ingannevole perché negli Store il consumatore compie una successiva scelta consapevole realizzando un'operazione di acquisto. Sulla base di tali considerazioni il TAR ha ritenuto lecita la Condotta A.

Riguardo alla Condotta B, il TAR osserva che non risulta corretta l'affermazione dell'Autorità secondo cui "*la pre-attivazione in questione determina, già di per sé, il trasferimento e l'utilizzo dei dati da parte di Apple, una volta che questi vengano generati, senza la necessità a tal fine di ulteriori passaggi in cui l'utente possa confermare o modificare la scelta pre impostata*". Ciò in quanto il TAR ha accertato che, all'atto della creazione dell'ID Apple e della personalizzazione degli Store, Apple non effettua alcuna attività di sfruttamento diretto dei dati personali degli utenti, i quali restano liberi di decidere se acquistare o meno.

In ultima analisi, secondo il TAR, nel caso di specie mancano gli elementi per considerare la pratica commerciale ingannevole e aggressiva, non avendo la Condotte A portata decettiva e non essendo la Condotta B in grado di produrre un "indebito condizionamento" del consumatore.

ANDREA MAREGA

***

Con **sentenza n. 15326 del 18.11.2022**, il TAR Lazio, Roma, sez. I, ha rigettato il ricorso di Google, confermando la legittimità del provvedimento del 16.11.2021 (caso PS11147) con cui l'AGCM aveva comminato alla società una sanzione di 10 milioni di euro complessivi, per due pratiche commerciali sleali limitative della libertà di scelta del consumatore medio.

La prima pratica (Condotta A), ritenuta scorretta, riguardava l'omessa informativa circa la raccolta e l'utilizzo dei dati personali degli utenti per finalità commerciali, sia nella fase di creazione dell'account Google (indispensabile per l'utilizzo di tutti i servizi offerti), sia durante l'utilizzo dei

servizi offerti da Google (ossia, Google Drive, Google Store, Google Play Store, Google Payments, Google Play Edicola, Google Play Musica, Google Maps, Google Search, Google Traduttore e YouTube).

La seconda pratica (Condotta B), ritenuta aggressiva, consisteva nella pre-impostazione del consenso degli utenti per acquisire i loro dati per le citate finalità commerciali nella fase di creazione dell'account Google. Questa pre-attivazione, secondo l'Autorità, consentiva il trasferimento e l'uso dei dati da parte di Google, una volta generati, senza la necessità di altri passaggi in cui l'utente potesse di volta in volta confermare o modificare la scelta pre-impostata dall'azienda.

Google ha impugnato il provvedimento dell'AGCM davanti al TAR, sollevando i seguenti motivi sostanziali:

1. assenza di una pratica ingannevole (Condotta A) in quanto, secondo Google, gli utenti sono stati adeguatamente informati della possibilità che i loro dati potessero essere utilizzati a fini commerciali;

2. mancanza dei presupposti per poter definire aggressiva la pratica consistente nella pre-impostazione del consenso degli utenti per acquisire i loro dati per le finalità commerciali nella fase di creazione dell'account Google (Condotta B), perché, secondo Google, gli utenti sono stati adeguatamente informati circa le-finalità dell'utilizzo dei loro dati;

2. quantificazione errata della sanzione in quanto, secondo Google, (i) l'AGCM non ha considerato come circostanza attenuante il fatto che Google avesse presentato impegni (respinti dalla stessa Autorità) e (ii) le due pratiche avrebbero dovuto essere qualificate come un'unica pratica.

Il TAR ha respinto tutti i motivi di ricorso promossi da Google.

Con riferimento al primo e al secondo motivo, il TAR ha ritenuto che Google avesse effettivamente utilizzato i dati degli utenti per fini commerciali senza che questi fossero stati adeguatamente informati.

In particolare, con riferimento alla Condotta A, secondo il TAR, le informazioni rese sia in sede di creazione dell'account Google, sia con riferimento all'accesso ai servizi di Google, non erano di immediata evidenza, in quanto posizionate in pagine raggiungibili attraverso link di consultazione meramente eventuali, come tali non idonei ad informare adeguatamente il consumatore sulla raccolta e sull'utilizzo a fini commerciali dei suoi dati.

Il TAR ha, inoltre, confermato la valutazione di aggressività della Condotta B, considerando che la pre-attivazione del consenso determinava di per sé il trasferimento e l'uso dei dati per scopi commerciali (una volta generati), senza che gli utenti ne fossero informati e senza la necessità di ulteriori passaggi da parte degli utenti. Inoltre, ad avviso del TAR, il processo di de-selezione del consenso pre-attivato non era né semplice né immediato.

Per quanto riguarda il terzo motivo, il TAR ha confermato la sanzione di 10 milioni di euro, tenuto conto della notevole dimensione economica del professionista quale leader mondiale nel settore, dell'ampia diffusione delle pratiche tramite internet, nonché del rifiuto dell'AGCM degli impegni presentati da Google e della necessità di mantenere le due pratiche (Condotta A e Condotta B) separate da un punto di vista strutturale e funzionale.

GIORGIA DIOTALLEVI

https://www.giustizia-amministrativa.it/