Juridical Observatory on Digital Innovation
Osservatorio Giuridico sulla Innovazione Digitale

DIRITTO E NUOVE TECNOLOGIE*

Rubrica di aggiornamento dell'OGID.

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

* 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 'Data Governance Act': Regolamento (UE) 2022/868 del 30 maggio 2022 sulla governance europea dei dati.

Il 30 maggio 2022, concludendo un lungo *iter* (v. notizia n. **4** sul numero **4/2021** di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2021/12/Osservatorio-1.pdf), i Presidenti del Parlamento Europeo e del Consiglio hanno sottoscritto il Regolamento (UE) 2022/868 relativo alla *governance* europea dei dati e che modifica il regolamento (UE) 2018/1724 ("***Data Governance Act***" o "**DGA**"), con il quale l'Unione Europea, nell'ambito della propria complessiva strategia sui dati - che contempla anche la direttiva c.d. *Open Data* (UE) 2019/1024, già attuata in Italia, e la proposta di regolamento c.d. *Data Act* (su cui v. rispettivamente le notizie nn. **2** e **4** nel numero **1/2022** di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf), si è posta l'obiettivo di creare un quadro armonizzato per gli scambi di dati, stabilendo alcuni requisiti di base per la *governance* dei dati.

Come emerge dal **Capo I** del *Data Governance Act* e, in particolare, dal relativo art. 1(1), il DGA si occupa di stabilire: *a)* le condizioni per il 'riutilizzo' di determinate categorie di dati detenuti da enti pubblici; *b)* un quadro di notifica e controllo per la fornitura di 'servizi di intermediazione dei dati'; *c)* un quadro per la registrazione volontaria delle entità che raccolgono e trattano i dati messi a disposizione a fini altruistici ('altruismo dei dati'); *d)* l'istituzione di un 'comitato europeo per l'innovazione in materia di dati'.

Il medesimo Capo I chiarisce che il DGA non crea alcun obbligo, per gli enti pubblici, di consentire il riutilizzo dei dati né li esenta dal rispetto degli obblighi di riservatezza imposti dal diritto dell'Unione o nazionale e che, inoltre, il *Data Governance Act* – per un verso – non pregiudica il diritto dell'UE (e nazionale) in materia di protezione dei dati personali e – per altro verso – lascia impregiudicata l'applicazione del diritto della concorrenza, nonché le competenze degli Stati membri in materia di sicurezza pubblica, difesa e sicurezza nazionale (art. 1(2)-(5) DGA).

L'art. 2 del DGA contiene, tra le altre, le seguenti definizioni:

- 'dati': "*qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva*" (art. 2, n. 1 DGA);
- 'riutilizzo': "*l'utilizzo di dati in possesso di enti pubblici da parte di persone fisiche o giuridiche a fini commerciali o non commerciali diversi dallo scopo iniziale nell'ambito dei compiti di servizio pubblico per i quali i dati sono stati prodotti, fatta eccezione per lo scambio di dati tra enti pubblici esclusivamente in adempimento dei loro compiti di servizio pubblico*" (art. 2, n. 2 DGA);
- 'dati personali': "*i dati personali quali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679* ["**GDPR**"]" (art. 2, n. 3 DGA);
- 'dati non personali': "*i dati diversi dai dati personali*" (art. 2, n. 4 DGA);
- 'consenso': "*consenso quale definito all'articolo 4, punto 11, del* [GDPR]" (art. 2, n. 5 DGA);
- 'autorizzazione': "*il conferimento agli utenti dei dati del diritto al trattamento dei dati non personali*" (art. 2, n. 6 DGA);
- 'interessato': "*l'interessato ai sensi dell'articolo 4, punto 1, del* [GDPR]" (art. 2, n. 7 DGA);
- 'titolare dei dati': "*una persona giuridica, compresi gli enti pubblici e le organizzazioni internazionali, o una persona fisica che non è l'interessato rispetto agli specifici dati in questione e che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli* (art. 2, n. 8 DGA);
- 'utente dei dati': "*una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e che ha diritto, anche a norma del* [GDPR] *in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali*" (art. 2, n. 9 DGA);
- 'condivisione dei dati': "*la fornitura di dati da un interessato o un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale di tali dati, sulla base di accordi volontari o del diritto dell'Unione o nazionale, direttamente o tramite un intermediario, ad esempio nel quadro di licenze aperte o commerciali, dietro compenso o a titolo gratuito*" (art. 2, n. 10 DGA);

- ‘servizio di intermediazione dei dati’: “*un servizio che mira a instaurare, attraverso mezzi tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e di utenti dei dati, dall’altro, anche al fine dell’esercizio dei diritti degli interessati in relazione ai dati personali*”; ad esclusione dei “*servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l’utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari e gli utenti dei dati*”, dei “*servizi il cui obiettivo principale è l’intermediazione di contenuti protetti da diritto d’autore*”, dei “*servizi utilizzati esclusivamente da un titolare dei dati per consentire l’utilizzo dei dati detenuti da tale titolare dei dati, oppure utilizzati da varie persone giuridiche all’interno di un gruppo chiuso,* […] *in particolare quelli aventi come obiettivo principale quello di garantire la funzionalità di oggetti o dispositivi connessi all’internet delle cose*” e dei “*servizi di condivisione dei dati offerti da enti pubblici che non mirano a instaurare rapporti commerciali*” (art. 2, n.11 DGA);
- ‘trattamento’: “*il trattamento quale definito all'articolo 4, punto 2, del* [GDPR] *in materia di dati personali o all'articolo 3, punto (2), del Regolamento (UE) 2018/1807* [regolamento sulla libera circolazione dei dati non personali] *in materia di dati non personali*” (art. 2, n.12 DGA);
- ‘accesso’: “*l'utilizzo dei dati, conformemente a specifici requisiti tecnici, giuridici o organizzativi, che non implica necessariamente la trasmissione o lo scaricamento di dati*” (art. 2, n.13 DGA);
- ‘servizi di cooperative di dati’: “*servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali*” (art. 2, n.15 DGA);
- ‘altruismo dei dati’: “*la condivisione volontaria dei dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l’uso dei loro dati non personali, senza la richiesta o ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l’assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l’agevolazione dell’elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento dei servizi pubblici, l’elaborazione di politiche pubbliche o la ricerca scientifica nell’interesse generale*” (art. 2, n. 16 DGA)
- ‘ambiente di trattamento sicuro’: “*l'ambiente fisico o virtuale e i mezzi organizzativi per garantire la conformità al diritto dell'Unione, quale il* [GDPR], *in particolare per quanto riguarda i diritti degli interessati, i diritti di proprietà intellettuale e la riservatezza commerciale e statistica, l'integrità e l'accessibilità, per garantire il rispetto del diritto dell'Unione e nazionale applicabile, e per consentire all'entità che fornisce l'ambiente di trattamento sicuro di determinare e controllare tutte le azioni di trattamento dei dati, compresi la visualizzazione, la conservazione, lo scaricamento, l'esportazione dei dati e il calcolo dei dati derivati mediante algoritmi computazionali*” (art. 2, n. 20 DGA).

Il **Capo II** del DGA si occupa di disciplinare il riutilizzo di determinate categorie di dati protetti detenuti da enti pubblici, questi ultimi definiti, all’art. 2, n. 17 DGA, come “*le autorità statali, regionali o locali, gli organismi di diritto pubblico* [come definiti al successivo n. 18 dell’art. 2 DGA], *o le associazioni formate da una o più di tali autorità oppure da uno o più di tali organismi di*

diritto pubblico") anzitutto subordinandolo al rispetto dei diritti dei soggetti ai quali è accordata la protezione. In particolare, l'art. 3(1) del DGA prevede che la disciplina del Capo II del DGA si applica ai dati detenuti da enti pubblici che sono protetti per motivi di *a)* riservatezza commerciale, compresi i segreti commerciali, professionali o d'impresa; *b)* riservatezza statistica; c) protezione dei diritti di proprietà intellettuale di terzi; o *d)* protezione dei dati personali, nella misura in cui tali dati non rientrano nell'ambito di applicazione della direttiva *Open Data* (UE) 2019/1024.

L'applicazione del medesimo Capo II, concernente il riutilizzo dei dati, è invece esclusa per i dati detenuti da imprese pubbliche, come definite all'art. 2, n. 19 DGA, da emittenti di servizio pubblico o dalle società da esse controllate, da enti culturali e di istruzione o, anche se detenuti da enti pubblici, laddove i dati siano protetti per ragioni di pubblica sicurezza, difesa o sicurezza nazionale (art. 3(2) DGA).

L'art. 4(1) del DGA pone poi un generale divieto di accordi o altre pratiche – relativamente al riutilizzo di dati detenuti da enti pubblici e rientranti nelle categorie di cui all'art. 3(1) del DGA – che siano volti a concedere diritti esclusivi o comunque a limitare la disponibilità di dati per il riutilizzo da parte di entità diverse dalle parti di tali accordi o pratiche. In deroga all'art. 4(1) del DGA, laddove risulti che la fornitura di un servizio o di un prodotto di interesse generale non sarebbe altrimenti possibile, è previsto che un "*diritto esclusivo di riutilizzo dei dati*" possa essere concesso – in via trasparente e pubblicando *online* il relativo atto amministrativo o accordo contrattuale con indicazione dei motivi in una forma conforme al pertinente diritto dell'Unione in materia di appalti pubblici – purché nella misura necessaria alla fornitura di tale servizio o prodotto di interesse generale. In ogni caso, la durata di tale diritto non può superare i dodici mesi.

L'art. 5 del DGA prevede poi che gli enti pubblici che hanno diritto di concedere o negare l'accesso al riutilizzo dei dati debbono rendere pubbliche le condizioni di tale riutilizzo (e la relativa procedura di richiesta), condizioni che devono essere "*non discriminatorie, trasparenti, proporzionate e oggettivamente giustificate in relazione alle finalità del riutilizzo e alle categorie e alla natura dei dati per i quali è consentito l'utilizzo*" (art. 5(1) e (2) DGA). Il riutilizzo dei dati può essere concesso anche dietro pagamento di una "*tariffa*" (art. 6 DGA), calcolata sulla base dei costi necessari per: la riproduzione, la fornitura, l'anonimizzazione, il mantenimento dell'ambiente di trattamento sicuro, l'acquisizione dell'eventuale diritto di consentire il riutilizzo da parte di terzi e l'assistenza ai riutilizzatori nel richiedere il consenso degli interessati.

Ancora, al Capo II del DGA viene prescritto a ciascuno degli Stati membri di introdurre uno "*sportello unico*" nazionale, affinché tutte le informazioni pertinenti relative all'applicazioni degli artt. 5 e 6 DGA siano disponibili e facilmente accessibili: in particolare, lo sportello unico "*è competente per il ricevimento delle richieste di informazioni e delle richieste di riutilizzo delle categorie di dati di cui all'art. 3, paragrafo 1, e le trasmette, ove possibile e opportuno con mezzi automatizzati, agli enti pubblici competenti o, se del caso, agli organismi competenti di cui all'articolo 7, paragrafo 1*" (art. 8(1) e (2) DGA).

Inoltre, è previsto che la Commissione istituisca "*un punto di accesso unico europeo che offre un registro elettronico consultabile dei dati disponibili presso gli sportelli unici nazionali e ulteriori informazioni su come richiedere i dati tramite tali sportelli unici nazionali*" (art. 8(4) DGA).

Relativamente al (diverso) sportello digitale unico previsto dal Regolamento (UE) 2018/1724 (che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE) n. 1024/2012), l'art. 36 del DGA modifica l'allegato II del medesimo Regolamento (UE) 2018/1724 inserendo tra le informazioni sull'avvio, gestione e chiusura delle imprese (ivi previste) anche la notifica del fornitore di servizi di intermediazione di dati (e la conferma della medesima notifica) e la registrazione come organizzazione per l'altruismo dei dati riconosciuta nell'Unione (e la conferma della medesima registrazione), previsti dal DGA.

Quanto alle richieste di riutilizzo dei dati, l'art. 9(1) del DGA prevede che – a meno che il diritto nazionale stabilisca termini inferiori – le decisioni degli enti pubblici o degli organismi competenti sul riutilizzo debbano avvenire entro due mesi dalla data di ricevimento della relativa richiesta, salva la possibilità di prorogare, in casi eccezionali, il termine per ulteriori 30 giorni, con relativo obbligo di comunicazione del ritardo e della sua motivazione. Il medesimo articolo prevede inoltre che ogni persona fisica o giuridica direttamente interessata dalle decisioni sul riutilizzo dei dati debba avere un "*effettivo diritto di ricorso*" contro di esse, secondo le modalità stabilite dalla legge nazionale di ciascuno Stato membro (art. 9(2) DFGA9.

Il **Capo III** contiene una serie di disposizioni sui requisiti applicabili ai servizi di intermediazione dei dati, informate alla finalità di accrescere la

fiducia nella condivisione dei dati e di ridurre i relativi costi di transazione.

L'art. 10(1) del DGA prevede che la fornitura di alcuni servizi di intermediazione dei dati (individuati nei "*servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati*", nei "*servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati*" e nei "*servizi di cooperative di dati*") sia soggetta al rispetto di una serie di condizioni, elencate nell'art. 12 del DGA, nonché al rispetto di una procedura di notifica disciplinata dall'art. 11 del DGA.

Quest'ultima disposizione stabilisce che i fornitori di servizi di intermediazione dei dati – anche stabiliti fuori dal territorio UE (nel qual caso, essi sono tenuti a nominare un rappresentante legale in uno degli Stati membri in cui offrono tali servizi) – che intendano fornire i servizi di cui all'art. 10 del DGA devono presentare una notifica all'autorità competente nazionale, designata dallo Stato membro ai sensi dell'art. 13 del DGA. Una volta presentata la notifica, i fornitori possono iniziare la loro attività in conformità alle disposizioni racchiuse nel Capo III del DGA.

Sulla conformità dei fornitori dei servizi di intermediazione dei dati ai requisiti di cui al Capo III dal *Data Governance Act* svolgono attività di monitoraggio e controllo le autorità competenti individuate da ciascuno Stato membro (art. 14(1) DGA). Ad esse, il *Data Governance Act* attribuisce una serie di rilevanti poteri. In particolare, tali autorità possono sottoporre ai fornitori di servizi di intermediazione di dati richieste di informazioni (art. 14(2) DGA) e, qualora constatino il mancato rispetto di uno o più dei requisiti di cui al Capo III del DGA, esse hanno il potere di notificare tale circostanza ai fornitori invitandoli ad esprimere le loro osservazioni entro 30 giorni (art. 14(3) DGA). Per il caso in cui venga rilevata una violazione, l'art. 14(4) DGA attribuisce inoltre a tali autorità il potere di ordinare la cessazione della violazione e di apportare modifiche ai servizi per ripristinare la conformità alle disposizioni del Capo III del DGA, di imporre sanzioni pecuniarie dissuasive nei confronti dei trasgressori e/o di avviare un procedimento giudiziario per la comminazione di una ammenda, nonché di ordinare il rinvio dell'inizio della fornitura dei servizi (se applicabile) ovvero una loro sospensione, fino a che non siano state apportate le richieste modifiche alle condizioni del servizio, ovvero una loro definitiva cessazione per il caso di gravi e reiterate violazioni e di mancata ottemperanza alle richieste di modifica comunicate dall'autorità, in quest'ultimo caso con conseguente cancellazione del fornitore dal registro dei fornitori di servizi di intermediazione di dati (art. 14(4) DGA).

L'art. 15 del DGA chiarisce infine che le disposizioni contenute nel Capo III non si applicano alle organizzazioni per l'altruismo dei dati (di cui si dirà in seguito) e alle altre entità senza scopo di lucro, nella misura in cui le loro attività consistano nel cercare di raccogliere, per obiettivi di interesse generale, dati messi a disposizione da persone fisiche o giuridiche sulla base dell'altruismo dei dati, a meno che tali organizzazioni ed entità non puntino a stabilire relazioni commerciali tra un numero indeterminato di interessati e titolari dei dati, da un lato, e utenti dei dati, dall'altro (art. 15 DGA).

All'altruismo dei dati è dedicato il **Capo IV** del DGA, il quale persegue l'obiettivo di facilitare i singoli individui e le imprese nel mettere volontariamente a disposizione dati per il bene comune. A tal fine, il *Data Governance Act* – che lascia notevole spazio all'autonomia organizzativa e tecnica dei singoli Stati membri dell'Unione (cfr. art. 16 DGA) – consente ai soggetti interessati di chiedere di essere iscritti ai "*registri pubblici delle organizzazioni per l'altruismo dei dati riconosciute*" (art. 17 DGA), tenuti dalle autorità competenti. Le autorità competenti per la registrazione delle organizzazioni per l'altruismo dei dati monitorano e controllano la conformità alle prescrizioni stabilite nel Capo V (art. 24 DGA) e sono dotate di poteri sostanzialmente corrispondenti a quelli riconosciuti, dall'art. 14 DGA, in capo alle autorità competenti per i fornitori di servizi di intermediazione.

I soggetti registrati, in possesso dei requisiti stabiliti all'art. 18 del DGA, sono riconosciuti in tutta l'UE, al fine di favorire la necessaria fiducia nell'altruismo dei dati e di incoraggiare i singoli e le imprese a 'donare' dati a tali organizzazioni, affinché possano essere utilizzati per apportare benefici sociali più ampi. Tra i requisiti imposti dall'art. 18 del DGA alle organizzazioni per l'altruismo dei dati riconosciute emerge, in particolare, l'adesione a un codice di condotta che sarà adottato dalla Commissione in collaborazione con gli *stakeholders* (artt. 18, lett. (e) e 22 DGA).

Il **Capo V** del DGA stabilisce i requisiti per il funzionamento delle autorità competenti dei singoli Stati membri, prevedendo – in particolare – che esse siano "*giuridicamente distinte e funzionalmente indipendenti da qualsiasi fornitore di servizi di intermediazione dei dati o organizzazione per l'altruismo dei dati riconosciuta*" e che le funzioni delle autorità competenti per i servizi di

intermediazione e quelle delle autorità competenti per le organizzazioni per l'altruismo possano "*essere svolte dalla stessa autorità*" (art. 26(1) DGA).

Tali autorità nazionali sono in ogni caso chiamate ad agire "*in maniera imparziale, trasparente, coerente, affidabile e tempestiva*", anche al fine di salvaguardare "*la concorrenza leale e la non discriminazione*" (art. 26(2) DGA).

Il Capo V del DGA contiene infine, agli artt. 28 e 29, alcune disposizioni relative al diritto degli interessati di presentare reclami contro le decisioni dei fornitori servizi di intermediazione dei dati e delle organizzazioni per l'altruismo dei dati riconosciute, e sul ricorso giurisdizionale nei confronti di tali decisioni.

Il **Capo VI** del DGA prevede l'istituzione del "*comitato europeo per l'innovazione in materia di dati*": un gruppo di esperti – costituito da rappresentanti delle autorità competenti ai fini del DGA, del Comitato europeo per la protezione dei dati (EDPB), del Garante europeo della protezione dei dati (EDPS), dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA), della Commissione, dal rappresentante dell'UE per le PMI (o da un rappresentante nominato dalla rete dei rappresentanti delle PMI) e da altri rappresentanti di organi pertinenti – che avrà, fra gli altri, il compito di consigliare e assistere la Commissione nello sviluppo di una prassi coerente degli enti pubblici e degli organismi competenti per il trattamento delle richieste di riutilizzo, nonché di una prassi coerente in materia di altruismo dei dati in tutta l'Unione.

Le norme di cui al **Capo VII** sono invece volte a proteggere dall'accesso e dal trasferimento internazionale illecito i dati detenuti da enti pubblici, da fornitori di servizi di intermediazione dei dati e da organizzazioni per l'altruismo dei dati riconosciute.

Al fine di garantire condizioni uniformi di esecuzione del DGA, il **Capo VIII** prevede la possibilità che la Commissione europea adotti atti di esecuzione del regolamento, assistita da un comitato, ai sensi del Regolamento (UE) n. 182/2011.

Infine, il **Capo IX** del DGA contiene una serie di disposizioni transitorie e finali, a norma delle quali gli Stati membri sono tenuti a stabilire le regole relative alle sanzioni da applicare in caso di violazione degli obblighi contenuti nel DGA, tenendo conto delle raccomandazioni del comitato europeo per l'innovazione in materia dei dati e dei criteri elencati in via non esaustiva all'art. 34(2) del DGA. Le sanzioni devono ogni caso essere "*effettive, proporzionate e dissuasive*" (art. 34(1) DGA).

Al fine di scongiurare il rischio di obsolescenza, insito in tale iniziativa legislativa, l'art. 35 del DGA prevede che la Commissione effettui una valutazione circa l'applicazione del DGA e presenti al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo una relazione sulle principali conclusioni tratte, entro trentanove mesi dall'entrata in vigore del medesimo DGA.

Il regolamento è entrato in vigore il 23 giugno 2022, e troverà applicazione a decorrere dal 24 settembre 2023 (art. 38 DGA).

RICCARDO ALFONSI

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R0868&from=EN

2. Approvato il 'Regolamento DLT': Regolamento (UE) 2022/858 del 30 maggio 2022 per un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito.

Il 30 maggio 2022 è stato approvato il regolamento (UE) 2022/858 del Parlamento europeo e del Consiglio (il "**Regolamento DLT**") che ha introdotto un "*regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito"* e che modifica i regolamenti (UE) n. 600/2014 (*Markets in Financial Instruments Regulation*: "**MiFIR**") e (UE) n. 909/2014 (*Central Securities Depositories Regulation*: "**CSDR**") e la direttiva 2014/65/UE (*Markets in Financial Instruments Directive II:* "**MiFID II**").

L'entrata in vigore del Regolamento DLT è stata fissata al 20 giugno 2022, tuttavia la maggior parte delle norme in esso contenute saranno applicabili dal 23 marzo 2023. Il Regolamento DLT costituisce uno dei tre su cui su poggerà il *framework* legislativo europeo sulla finanza digitale (il *digital finance package*). Gli altri due pilastri sono rappresentati dalle proposte di regolamento sulla resilienza operativa digitale (*Digital Operational Resilence Act*: "**DORA**") e sui *Markets in Crypto-Assets* ("**Regolamento MiCA**": su cui vedi la notizia successiva *sub* **3** in questo numero di questa Rubrica), entrambi ancora in corso di approvazione.

Il Regolamento DLT istituisce un regime temporaneo (o "pilota") per le infrastrutture di mercato che operano attraverso una tecnologia a registro distribuito ("**DLT**") con le dichiarate finalità di testare tali tecnologie e consentire lo

sviluppo delle cripto-attività che rientrano nella definizione di strumenti finanziari, come modificata dal medesimo Regolamento DLT, e di garantire al contempo un livello elevato di tutela degli investitori, l'integrità del mercato, la stabilità finanziaria e la trasparenza. Il regime "pilota" contempla l'esenzione temporanea di alcuni requisiti specifici previsti dall'Unione in materia di servizi finanziari. È previsto che tale regime sarà soggetto ad un "riesame" nell'anno 2026, a seguito di una relazione sul funzionamento e sui rischi del sistema pilota ad opera della Commissione europea, la quale, sulla base di un'analisi costi/benefici, stabilirà se il regime pilota potrà essere prorogato (per un periodo massimo di tre anni), e/o esteso ad altre tipologie di strumenti finanziari, modificato, reso permanente o soppresso.

Una delle novità più significative introdotte dal Regolamento DLT riguarda la modifica della definizione di strumento finanziario. L'art. 18 del Regolamento DLT, andando a modificare la definizione di strumento finanziario contenuta all'art. 4, paragrafo 1, punto 15 della direttiva 2014/65/UE, definisce strumento finanziario "*qualsiasi strumento riportato nella sezione C dell'allegato I, compresi gli strumenti emessi mediante tecnologia a registro distribuito*". Lo "*strumento finanziario DLT*" viene a sua volta definito nel Regolamento DLT come "*strumento finanziario emesso, registrato, trasferito e stoccato mediante la tecnologia a registro distribuito*". Gli strumenti finanziari DLT dovrebbero essere limitati alle azioni, alle obbligazioni e alle quote di organismi di investimento collettivo. In aggiunta, come ricorderemo più sotto, è previsto un limite al valore di mercato aggregato degli strumenti finanziari DLT ammessi alla negoziazione o registrati in un'infrastruttura di mercato DLT ai fini di preservare la stabilità finanziaria.

Il Regolamento DLT definisce come "registro distribuito" qualunque *"archivio di informazioni in cui sono registrate le operazioni e che è condiviso da una serie di nodi di rete DLT ed è sincronizzato tra di essi, mediante l'utilizzo di un meccanismo di consenso"*; definisce "nodo di rete DLT" "*un dispositivo o un'applicazione informatica che è parte di una rete e che detiene una copia completa o parziale delle registrazioni di tutte le operazioni eseguite tramite il registro distribuito*"; ed infine definisce "meccanismo di consenso" "*le regole e le procedure con cui si raggiunge un accordo, tra i nodi di rete DLT, sulla convalida di un'operazione*". La definizione di matrice europea è più estesa e inclusiva di quella nazionale contenuta nel Decreto Legge n. 135 del 14 dicembre 2018 che, con un maggior dettaglio definitorio (oggetto di non poche critiche da parte degli esperti di settore) aveva già introdotto per la prima volta, in Italia, la definizione di «tecnologia basata su registro distribuito» consistente in "*tecnologie e protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili"*.

Il Regolamento DLT, a seguito della (ri)definizione della nozione di strumento finanziario, introduce un regime giuridico unitario per le "infrastrutture di mercato DLT", ovverosia per *i)* i sistemi multilaterali di negoziazione DLT (o "**MTF DLT**"), *ii)* i sistemi di regolamento DLT (o "**SS DLT**") e *iii)* i sistemi di negoziazione e regolamento DLT (o "**TSS DLT**").

L'MTF DLT è quel sistema multilaterale di negoziazione che ammette alla negoziazione solo strumenti finanziari DLT. L'SS DLT è un sistema che regola operazioni in strumenti finanziari DLT contro pagamento o consegna. Infine, un TSS DLT è un fornitore di servizi che combina sia i servizi di negoziazione tipicamente prestati da un MTF DLT, sia i servizi di regolamento dei SS DLT.

L'ambito applicativo del Regolamento DLT, dal punto di vista oggettivo, risulta speculare e complementare all'ambito applicativo destinato ad esser disciplinato dal Regolamento MiCA (sul quale v. più in particolare la notizia successiva *sub* **3** in questo numero di questa Rubrica). Mentre il Regolamento DLT si applica a strumenti finanziari DLT e ai gestori di infrastrutture DLT che ammettono la negoziazione o il regolamento e la registrazione di strumenti finanziari basati su tecnologia DLT, il Regolamento MiCA non si applica, specularmente, ai *cripto-asset* che siano anche strumenti finanziari. Ne consegue che le criptovalute e i *cripto-asset* non qualificabili come strumenti finanziari (ad es. le *stablecoin*, i *token* di moneta elettronica, gli *utility token* etc.) saranno disciplinati dal Regolamento MiCA e sottratti all'applicazione del Regolamento DLT.

Quanto ai requisiti di ammissibilità alla negoziazione o alla registrazione su una infrastruttura di mercato DLT, degna di nota è la disciplina contenuta nell'art. 3 del Regolamento DLT. Gli strumenti finanziari DLT potranno essere ammessi alla negoziazione o registrati su un'infrastruttura di mercato DLT a condizione che, al momento dell'ammissione alla negoziazione o della registrazione in un registro distribuito, gli

strumenti finanziari DLT ricadano in una delle seguenti categorie: a) azioni emesse da un emittente con capitalizzazione di mercato inferiore a Euro 500 milioni; b) obbligazioni o altre forme di debito cartolarizzato, o strumenti del mercato monetario con un'entità di emissione inferiore a Euro 1 miliardo; c) quote di organismi di investimento collettivo il cui valore di mercato delle attività gestite sia inferiore a Euro 500 milioni (art. 3, comma 1).

Accanto a tali limiti quantitativi inerenti al valore degli strumenti emessi, ulteriori limiti riguardano l'infrastruttura di mercato: il valore di mercato aggregato di tutti gli strumenti finanziari DLT ammessi alla negoziazione o registrati su un'infrastruttura di mercato DLT non dovrà superare i 6 miliardi di Euro al momento dell'ammissione alla negoziazione o della registrazione iniziale di un nuovo strumento finanziario DLT (art. 3, comma 2).

L'ammissione o la registrazione di nuovi strumenti finanziari DLT sarà preclusa laddove, per effetto dell'ammissione o della registrazione, venisse superato il valore massimo.

Laddove il valore di mercato complessivo degli strumenti finanziari DLT già negoziati o registrati dovesse superare i 9 miliardi di Euro (a prescindere dall'ammissione di nuovi strumenti, come ad esempio, per effetto dell'aumento di valore di mercato degli strumenti DLT negoziati o registrati), il gestore dell'infrastruttura di mercato DLT sarà tenuto ad attivare un'apposita *"strategia di transizione"* (art. 3, comma 3) prevista dall'art. 7 (v. *infra*).

Per garantire il monitoraggio delle soglie massime, il gestore dell'infrastruttura di mercato DLT sarà tenuto a *i)* calcolare mensilmente il valore di mercato aggregato medio degli strumenti finanziari DLT negoziati o registrati sulla propria infrastruttura e *ii)* presentare relazioni mensili alla propria autorità nazionale di vigilanza da cui risulti che tutti gli strumenti finanziari DLT ammessi alla negoziazione o registrati nell'infrastruttura di mercato DLT non superano le soglie massime.

Gli istituti finanziari già autorizzati (imprese di investimento, gestori di sistemi MTF, depositari centrali di titoli etc.) possono chiedere un'autorizzazione specifica per estendere la loro attività anche agli strumenti finanziari DLT e operare, quindi, come gestori di infrastrutture di mercato DLT.

Gli articoli 8, 9 e 10 del Regolamento DLT contengono la disciplina di dettaglio dei procedimenti per ottenere l'autorizzazione come gestore di MTF DLT, di SS DLT o di TSS DLT. Tuttavia, data la natura assimilabile ad una forma di *regulatory sand box* introdotta dal Regolamento DLT, nel caso delle infrastrutture di mercato DLT, l'autorizzazione è temporanea e limitata a un periodo massimo di sei anni.

L'autorizzazione concessa a un gestore di un'infrastruttura di mercato DLT dovrebbe seguire le stesse procedure previste dalla MiFID II e dal CSDR. La concessione dell'autorizzazione e la vigilanza in generale è rimessa all'Autorità competente. L'ESMA può fornire un parere non vincolante sulle esenzioni richieste o sull'adeguatezza della tecnologia. Le autorità competenti dovranno poi trasmettere a loro volta all'ESMA le informazioni raccolte e le relazioni ricevute dai gestori delle infrastrutture di mercato DLT.

In ogni caso, l'accesso al mercato delle infrastrutture DLT è aperto sia agli *incumbent* già operanti come gestori di MTF o come depositari centrali di titoli, sia a soggetti che intendano ottenere contestualmente un'autorizzazione ai sensi del Regolamento DLT e un'autorizzazione in qualità di impresa di investimento o di depositario centrale di titoli.

Le infrastrutture di mercato DLT dovranno essere sottoposte a requisiti aggiuntivi particolarmente stringenti, soprattutto in relazione agli obblighi informativi. Il Regolamento DLT prevede, tra gli altri, l'obbligo di messa a disposizione del pubblico di informazioni scritte sulle regole che presidiano la loro operatività e i loro gestori, comprese la disciplina dei diritti, dei requisiti, delle responsabilità e degli obblighi dei gestori delle infrastrutture di mercato DLT, nonché quelli dei membri, dei partecipanti, degli emittenti e dei clienti che utilizzano le loro infrastrutture di mercato DLT, ed altre informazioni rilevanti anche sulla 'strategia di uscita' nel caso in cui il regime pilota sia sospeso.

I gestori di infrastrutture DLT dovranno inoltre osservare diversi requisiti organizzativi.

Innanzi tutto, per quanto concerne le infrastrutture tecniche, i gestori dovranno garantire che tutti i dispositivi informatici e cibernetici relativi all'uso della loro tecnologia DLT siano proporzionati alla natura, alla portata e alla complessità delle loro attività. I dispositivi dovranno assicurare la continuità e la costante trasparenza, disponibilità, affidabilità e sicurezza dei servizi e delle attività, compresa l'affidabilità degli *smart contract* utilizzati nell'infrastruttura di mercato DLT.

Tali dispositivi dovranno inoltre garantire l'integrità, la sicurezza e la riservatezza di tutti i dati memorizzati dai gestori in questione, nonché che tali dati siano disponibili e accessibili.

I gestori delle infrastrutture DLT saranno tenuti ad adottare procedure specifiche di gestione del rischio operativo per i rischi derivanti dall'uso della tecnologia a registro distribuito e delle cripto-attività.

Degna di nota è l'attribuzione alle autorità nazionali di vigilanza di un pervasivo potere ispettivo per valutare l'affidabilità dei dispositivi informatici e cibernetici di un'infrastruttura di mercato DLT. Nel caso in cui l'autorità di vigilanza chieda di esercitare una verifica, essa dovrà nominare un revisore indipendente. È stato però previsto che, in caso di verifiche disposte dalle autorità di vigilanza, il costo della verifica (incluso quindi anche il costo dell'esperto) ricada sul gestore dell'infrastruttura di mercato DLT (art. 7, comma 4).

L'art. 7, comma 5 stabilisce che qualora un gestore offra il servizio di custodia dei fondi, delle garanzie o degli strumenti finanziari DLT nonché i servizi di accesso a tali *asset* (anche sotto forma di chiavi crittografiche), il gestore deve adottare dispositivi adeguati per impedire l'uso di tali beni per suo conto e senza un previo esplicito consenso scritto del titolare degli asset.

Sempre l'art. 7, comma 5 prescrive la segregazione e la separazione degli asset stabilendo che i gestori delle infrastrutture DLT devono tenere separati i fondi, le garanzie reali e gli strumenti finanziari DLT dei clienti e degli emittenti da quelli del gestore, nonché da quelli di clienti o altri emittenti.

Nella prospettiva dell'incremento della fiducia degli investitori verso le nuove forme di investimento in strumenti finanziari DLT, l'art. 7, comma 6 prevede poi che in caso di perdita dei fondi, delle garanzie reali o degli strumenti finanziari DLT, il gestore dell'infrastruttura DLT è responsabile della perdita fino al valore di mercato dell'attività persa.

In termini civilistici, parrebbe che l'espressione *"fino al valore"* operi come limitazione di responsabilità al solo danno emergente (*i.e.* la perdita del valore degli asset) e non copra il lucro cessante.

Inoltre, il gestore dell'infrastruttura DLT è esente da responsabilità se dimostra che la perdita è dovuta a un evento esterno che sfugge al suo ragionevole controllo, le cui conseguenze sarebbero state inevitabili nonostante ogni ragionevole sforzo per evitarlo. Questa fattispecie di esonero da responsabilità potrebbe prestare il fianco ad alcuni problemi applicativi a causa della compresenza di diversi concetti generali (ad es. *"evento esterno", "ragionevole controllo"* o *"ragionevole sforzo"*).

I gestori dell'infrastruttura di mercato DLT dovranno poi istituire dispositivi trasparenti e adeguati per garantire la tutela degli investitori e istituire altresì meccanismi di gestione dei reclami dei clienti e procedure di ricorso e compensazione nel caso in cui gli investitori subiscano perdite dovute a eventi tecnici.

L'autorità di vigilanza competente potrà decidere, caso per caso, di esigere ulteriori garanzie prudenziali da parte del gestore di un'infrastruttura di mercato DLT sotto forma di fondi propri o di polizze assicurative.

Una delle novità più interessanti offerta dal Regolamento DLT, è costituito dalla possibilità, per i gestori di infrastrutture DLT, di chiedere ed ottenere specifiche esenzioni dall'osservanza di altre normative regolanti il mercato finanziario.

Tra le disposizioni più rilevanti in materia di esenzioni introdotte dal Regolamento DLT, si prevede per i gestori MTF DLT un'esenzione all'obbligo di intermediazione previsto da MiFID II. In particolare, si prevede che le autorità competenti, su richiesta del gestore MTF, possano consentire a un accesso diretto di investitori non professionali, a patto che siano predisposte adeguate misure di protezione degli investitori e che questi soddisfino determinate condizioni.

Per i depositari centrali di titoli come definiti dal MiFIR ("**CSD**") che gestiscono un SS DLT, invece, si prevede un'esenzione dalle norme facenti riferimento a termini di "forma dematerializzata", "conto titoli" o "ordini di trasferimento". In particolare, un CSD può beneficiare di tale esenzione nella misura in cui dimostri come l'uso di un conto titoli sia incompatibile con l'uso di tecnologia DLT e adotti misure compensative. Specifiche esenzioni sono anche previste a determinate condizioni dall'obbligo di autorizzazione per l'esternalizzazione di un servizio o un'attività, all'obbligo di intermediazione ai fini di consentire accesso diretto ai sistemi di regolamento e di consegna gestiti da un CSD per i CSD che gestiscono un SS DLT, e, da ultimo, al regolamento delle operazioni in moneta di banca centrale.

BENEDETTO COLOSIMO

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022R0858

3. Verso il Regolamento MiCA: l'accordo del 30 giugno 2022 tra il Parlamento europeo e il Consiglio sul regolamento europeo sui mercati di cripto-attività.

Il 30 giugno 2022 è stato comunicato il raggiungimento di un accordo provvisorio (l'"**Accordo**") tra la presidenza del Consiglio e il Parlamento europeo in merito alla proposta di regolamento relativo ai mercati delle cripto-attività (il "**Regolamento MiCA**"), concludendo i triloghi iniziati nel marzo 2022. Il Regolamento MiCA (anche "MiCAR": *Markets in Crypto-Assets Regulation*) delinea una disciplina per gli emittenti di cripto-attività non garantite e di *stablecoin* e per i prestatori di servizi in cripto-attività. La proposta in merito era stata presentata dalla Commissione europea il 24 settembre 2020 (v. notizia n. **2** nel numero **4/2020** in questa Rubrica).

Tre sono i punti chiave dell'Accordo. In primo luogo, si ha la regolamentazione dei rischi connessi alle cripto-attività. Scopo del Regolamento MiCA sarà la protezione degli investitori in cripto-attività. In particolare, si prevede la responsabilità dei fornitori di servizi per le cripto-attività in caso di perdita delle cripto-attività degli investitori. Il Regolamento si propone di proibire anche ogni forma di abuso di mercato e, in particolare, di manipolazione del mercato e di abuso di informazioni privilegiate. Particolare attenzione sarà anche data all'impronta ambientale e climatica delle cripto-attività, rispetto a cui gli emittenti e i prestatori di servizi in cripto-attività dovranno fornire specifiche informazioni. Al riguardo, progetti di norme tecniche di regolamentazione saranno elaborati dall'ESMA. In aggiunta, la Commissione europea presenterà entro due anni una relazione sull'impatto ambientale delle cripto-attività. Il Regolamento MiCA non contiene disposizioni specifiche sull'antiriciclaggio per evitare sovrapposizioni con la normativa in merito. Si applicheranno, quindi, ai fornitori di servizi per le cripto-attività situati in paesi terzi "ad alto rischio" gli obblighi rafforzati previsti dal quadro regolamentare vigente. Il Regolamento MiCA prevederà solamente che l'EBA debba tenere un registro pubblico dei fornitori di servizi per le cripto-attività non conformi al quadro vigente.

In secondo luogo, l'Accordo prevede novità per gli *stablecoin*. In particolare, la disciplina si presenta più severa rispetto alla versione iniziale della proposta, anche alla luce dei recenti avvenimenti nel relativo mercato. In particolare, l'Accordo prevede che gli emittenti di *stablecoin* debbano costituire una riserva di attività sufficientemente liquide in un rapporto 1:1. Ciò al fine di garantire in qualsiasi momento la redimibilità alla pari. Specifiche disposizioni saranno previste per assicurare una liquidità minima adeguata. All'EBA ne sarà affidata la supervisione. Con riferimento ai *token* collegati ad attività basati su valuta non europea, il volume delle transazioni su base giornaliera sarà limitato per preservare la sovranità monetaria. In aggiunta, gli emittenti di *token* collegati ad attività dovranno avere una sede legale nell'Unione Europea.

Da ultimo, secondo l'Accordo, il Regolamento MiCA conterrà norme per i fornitori di servizi per le cripto-attività. In particolare, questi saranno soggetti ad autorizzazione per operare all'interno dell'UE. Siccome la supervisione e la vigilanza sarà affidata alle Autorità nazionali competenti, queste dovranno procedere al rilascio dell'autorizzazione entro tre mesi. Le Autorità nazionali competenti dovranno comunque trasmettere regolarmente informazioni pertinenti all'ESMA, alla quale sarà affidato un ruolo di coordinamento per i fornitori di servizi per le cripto-attività con un'operatività rilevante.

L'accordo provvisorio dovrà ora essere approvato dal Consiglio e dal Parlamento europeo. Ancora numerosi fenomeni rimangono non disciplinati dal Regolamento, tra cui *decentralised finance*, *crypto lending* e *non-fungible token*. In merito a quest'ultimi, però, pur essendo essi stati esclusi generalmente dall'ambito di applicazione, il Regolamento MiCA ne prevede la disciplina nel caso in cui rientrino nelle categorie di cripto-attività esistenti. Secondo l'Accordo, inoltre, la Commissione Europea dovrà preparare entro 18 mesi una valutazione globale sui *non-fungible token* (NFT) e presentare una proposta legislativa specifica nel caso lo ritenga necessario.

ALICE FILIPPETTA

https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/

4. La sentenza della Corte di Giustizia dell'Unione europea del 26 aprile 2022 sul ricorso proposto dalla Polonia avverso alcune disposizioni dell'art. 17 della direttiva (UE) 2019/790 sul copyright nel mercato unico digitale (Causa C-401/19)

Con la sentenza della Corte di giustizia dell'Unione Europea (la "**CGUE**" o la "**Corte**") del 26 aprile 2022 nella causa C-401/19 Polonia c. Parlamento e Consiglio (la "**Sentenza**"), la CGUE ha respinto il ricorso proposto dalla Repubblica di Polonia avverso l'articolo 17 della direttiva (UE) 2019/790 del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che

modifica le direttive 96/9/CE e 2001/29/CE (di seguito "**direttiva CDSM**" o "**CDSMD**": *Copyright in Digital Single Market Directive*) dichiarando che l'art. 17 CDSMD prevede adeguate garanzie per assicurare il rispetto del diritto alla libertà di espressione e di informazione da esso giustificatamente limitato a tutela del diritto d'autore, nonché un giusto equilibrio tra i due diritti in questione.

La Sentenza è stata emanata dopo che la direttiva CDSM è stata recepita in Italia con il Decreto Legislativo 177 dell'8 novembre 2021 entrato in vigore il 12 dicembre 2021 (il "**Decreto di recepimento della direttiva CDSM**") che ha apportato numerose modifiche alla legge italiana sul diritto di autore (Legge 22 aprile 1941 n. 633, di seguito "**l.a.**") (sul Decreto di recepimento della direttiva CDSM v. la notizia n. **1** nel numero **1/2022** di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf).

La questione principale sollevata dalla Polonia di fronte alla CGUE riguarda la validità delle misure preventive formulate in termini di obblighi di cosiddetti "massimi sforzi" ("*best efforts*" della versione in lingua inglese inglese della CDSMD) richieste dalle disposizioni di cui all'art. 17, paragrafo 4, lettere b) e c), in fine, della direttiva CDSM, alla luce del diritto alla libertà di espressione e di informazione riconosciuto dall'articolo 11 della Carta dei diritti fondamentali dell'Unione europea (di seguito la "**Carta**" o "**CDFUE**"). In subordine, la Polonia ha chiesto alla Corte di annullare l'art. 17 CDSMD nella sua interezza per il caso in cui la Corte avesse ritenuto che le citate disposizioni dell'art. 17 CDSMD non siano separabili dalle altre disposizioni del medesimo articolo.

Il Parlamento europeo e il Consiglio dell'UE hanno chiesto il rigetto delle conclusioni della Repubblica di Polonia. Il Regno di Spagna, la Repubblica francese, la Repubblica portoghese e la Commissione europea sono intervenute a sostegno delle conclusioni del Parlamento e del Consiglio.

L'articolo 17 CDSMD in questione si applica agli *Online Content-Sharing Service Providers* (di seguito "**OCSSP**") definiti ai sensi dell'art. 2(6) della direttiva CDSM come prestatori di servizi di condivisione di contenuti *online* il cui scopo principale (o uno dei principali scopi), è quello di memorizzare e dare accesso al pubblico a grandi quantità di opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti, che il servizio organizza e promuove a scopo di lucro.

In estrema sintesi, l'articolo 17 CDSMD stabilisce che gli OCSSP compiono atti di comunicazione al pubblico quando danno accesso a opere o altri materiali caricati dai loro utenti protetti dal diritto d'autore, e che, di conseguenza, questi fornitori diventano in principio direttamente responsabili dei caricamenti. L'art. 17(3) CDSMD esclude infatti espressamente l'applicazione per tali OCSSP del cd. "*safe harbour*" che stabilisce un'esenzione di responsabilità per l'attività degli *hosting provider* (ai sensi dell'articolo 14(1) della Direttiva 2000/31/CE, c.d. direttiva sul commercio elettronico) e introduce al contempo un complesso insieme di norme per regolamentare gli OCSSP introducendo un particolare meccanismo di esenzione dalla responsabilità (art. 17(4) CDSMD) e una serie di misure di attenuazione e salvaguardia.

Il meccanismo di esenzione dalla responsabilità di cui all'articolo 17(4) della direttiva CDSM – che forma più da vicino oggetto dell'esame della Corte nella Sentenza - comprende una serie di obblighi cumulativi di "*massimi sforzi*" ("*best efforts*" nella versione in lingua inglese della direttiva CDSM) previsti in capo agli OCSSP per: *(a)* ottenere un'autorizzazione dai titolari dei diritti di cui all'articolo 3, paragrafi 1 e 2, della direttiva 2001/29/CE, ad esempio mediante la conclusione di un accordo di licenza; *(b)* garantire l'indisponibilità di specifici contenuti protetti che sono state adeguatamente notificati dai titolari dei diritti; e *(c)* mettere in atto meccanismi di notifica e rimozione/sospensione.

Come osservazione preliminare, va notato che la CGUE ha seguito nella Sentenza in gran parte le indicazioni dell'Avvocato Generale ritenendo che l'articolo 17 CDSMD possa essere valutato solo nella sua interezza, il che significa che le lettere b) e c), dell'art.17(4) CDSMD non dovrebbero essere valutate separatamente (punto 21 della Sentenza).

La Corte ha confermato che l'articolo 17(4)(b) CDSMD impone agli OCSSP di effettuare *de facto* un esame preventivo dei contenuti caricati nei casi in cui i titolari dei diritti abbiano fornito "*informazioni pertinenti e necessarie*"(punto 53 della Sentenza).

È importante notare che la Corte riconosce che, a seconda dell'entità del compito (ossia "*a seconda del numero di file caricati e del tipo di materiale protetto in questione, ed entro i limiti stabiliti dall'articolo 17, paragrafo 5* [CDSMD]"), il controllo dei contenuti caricati da parte degli OCSSP richiede "*strumenti automatici di riconoscimento e filtraggio*" (punto 54 della Sentenza).

Pertanto, in alcuni casi - e sicuramente per le piattaforme più grandi (ad esempio YouTube e Meta) - il filtraggio automatico dei contenuti è necessario per rispettare gli obblighi di massimi

sforzi (*best efforts*) di cui all'articolo 17(4) della direttiva CDSM.

Per la Corte, tali controlli e filtri preventivi possono limitare un importante mezzo di diffusione dei contenuti *online*. La CCGUE ha infatti riconosciuto nella Sentenza che l'art. 17(4) CDSMD comporta effettivamente una limitazione all'esercizio del diritto alla libertà di espressione e di informazione degli utenti di tali servizi di condivisione di contenuti, come garantito dall'art. 11 della Carta e dall'art. 10 della CEDU (punti 55, 58, 82 della Sentenza).

Tuttavia, la Corte ritiene che tale limitazione sia giustificata rispetto all'obiettivo legittimo perseguito dall'art. 17 CDSMD, ossia quello di garantire un elevato livello di protezione ai titolari dei diritti ai sensi dell'art. 17, par. 2, della Carta e alla luce del criterio di cui all'art. 52, par. 1, della Carta, che richiede che qualsiasi limitazione all'esercizio dei diritti e delle libertà riconosciuti dalla Carta stessa sia prevista dalla legge e rispetti l'essenza di tali diritti e libertà.

Nella Sentenza, la Corte ha argomentato che, sebbene il meccanismo alternativo proposto dalla Polonia, in base al quale dovrebbero essere imposti agli OCSSP solo gli obblighi di cui alla lettera a) e all'inizio della lettera c) dell'articolo 17(4) CDSMD, costituirebbe effettivamente una misura meno restrittiva per quanto riguarda l'esercizio del diritto alla libertà di espressione e di informazione, tale meccanismo alternativo non sarebbe tuttavia altrettanto efficace in termini di tutela dei diritti di proprietà intellettuale rispetto al meccanismo adottato dal legislatore dell'UE (punto 84 della Sentenza).

La Corte ha poi esposto sei argomenti a supporto della sua decisione, per dimostrare che la limitazione imposta dall'articolo 17(4) CDSMD al diritto di libertà di espressione e di informazione, oltre ad essere giustificata, non lo limita in modo sproporzionato (punti 85 e segg. della Sentenza).

In primo luogo la Corte ha dichiarato che il legislatore dell'UE ha stabilito limiti chiari e precisi per le misure preventive, vietando, in particolare, le misure che filtrano e bloccano i contenuti leciti durante il caricamento. A questo proposito, la CGUE ha osservato nella Sentenza che un sistema di filtraggio che rischi di non distinguere adeguatamente tra contenuti leciti e illeciti (anche avuto riguardo alle particolarità degli ordinamenti nazionali) non sarebbe conforme ai requisiti dell'articolo 17 CDSMD e all'equo bilanciamento tra diritti e interessi concorrenti (punti 85-86 della Sentenza).

In secondo luogo, la Corte ha osservato che l'art. 17(7) CDSMD impone agli Stati membri di provvedere affinché gli utenti in ogni Stato membro siano autorizzati a caricare e a mettere a disposizione contenuti generati da loro stessi per scopi specifici come citazione, critica, rassegna, caricatura, parodia o pastiche (rendendo così obbligatorie tali eccezioni e limitazioni, prima previste come facoltative dall'art. 5 della direttiva 2001/29), e che gli utenti debbano essere informati dagli OCSSP della possibilità di utilizzare le opere conformemente alle eccezioni o limitazioni al diritto d'autore e ai diritti connessi previste dal diritto dell'Unione (art. 17(9) CDSMD) (punti 87-88 della Sentenza).

In terzo luogo, la Corte ha argomentato che il nuovo regime di responsabilità degli OCSSP relativo ai servizi da loro offerti richiede pur sempre la fornitura da parte dei titolari dei diritti di "*informazioni pertinenti e necessarie*" (art. 17(4)(b) CDSMD) o di una "*notifica sufficientemente motivata*" (art. 17(4)(c), in fine CDSMD), vale a dire una condizione preliminare che la Corte ritiene "*protegga l'esercizio del diritto alla libertà di espressione e di informazione degli utenti che utilizzano legittimamente tali servizi*" (punto 89 della Sentenza).

In quarto luogo, al punto 90 della Sentenza, la Corte ha sottolineato come l'art. 17(8) CDSMD espressamente sancisca che la sua applicazione non deve comportare alcun obbligo generale di monitoraggio. Si tratta, osserva la CGUE, di "*un'ulteriore salvaguardia per garantire il rispetto del diritto alla libertà di espressione e di informazione degli utenti degli* [OCSSP]", nel senso che tali fornitori "*non possono essere obbligati a impedire il caricamento e la messa a disposizione del pubblico di contenuti che, per essere ritenuti illeciti, richiederebbero una valutazione indipendente dei contenuti da parte loro alla luce delle informazioni fornite dai titolari dei diritti e di eventuali eccezioni e limitazioni al diritto d'autore*". In quanto tali, gli OCSSP non devono essere costretti a effettuare "*una valutazione indipendente del contenuto*" per determinarne la liceità, ad esempio confrontando le informazioni fornite dai titolari dei diritti con le eccezioni applicabili (applicando tra l'altro per analogia la sentenza della CGUE nella causa C-18/18 Glawischnig-Piesczek, punti 41-46, richiamata nella stessa Sentenza).

In quinto luogo, la Corte ha argomentato che le diverse garanzie procedurali introdotte dall'art. 17(9) CDSMD sono adeguate ad affrontare le situazioni di disabilitazione all'accesso dei contenuti o la rimozione di contenuti (punti 93-95 della Sentenza).

In sesto luogo, la Corte ha osservato che, ai sensi dell'art. 17(10) CDSMD, la Commissione

europea ha condotto dialoghi con gli *stakeholders* e ha elaborato orientamenti per integrare il sistema di garanzie previsto dall'art. 17(7), (8) e (9), che, tra l'altro tengono conto in modo particolare della necessità di bilanciare i diritti fondamentali e l'uso di eccezioni e limitazioni e forniscono alle organizzazioni di utenti l'accesso a informazioni adeguate da parte degli OCSSP sul funzionamento delle loro pratiche in relazione all'articolo 17(4) CDSMD (punto 96 della Sentenza).

La Corte conclude dichiarando che l'art. 17 CDSMD offre garanzie adeguate a garantire il diritto alla libertà di espressione e di informazione degli utenti e un giusto equilibrio tra tale diritto degli utenti e il diritto alla proprietà intellettuale (punto 98 della Sentenza): ciò in quanto, la Corte osserva che l'obbligo per i fornitori di servizi di condivisione di contenuti *online* di controllare i contenuti che gli utenti intendono caricare sulle loro piattaforme prima della loro diffusione al pubblico, derivante dal regime specifico di responsabilità introdotto dall'articolo 17, paragrafo 4, della direttiva 2019/790, e segnatamente dalle condizioni di esonero previste all'articolo 17, paragrafo 4, lettera b), e lettera c), in fine, di quest'ultima, è accompagnato dalle garanzie necessarie per assicurare la sua compatibilità con la libertà di espressione e d'informazione.

Se la Sentenza è stata molto netta nel respingere *in toto* le contestazioni mosse dalla Polonia all'art. 17 CDSMD, al contempo, però, la Corte ha chiarito che la medesima Sentenza riguarda esclusivamente la direttiva CDSM e non anche le normative nazionali di recepimento che rimangono soggetto al normale e stretto scrutinio di legittimità (punto 71 della Sentenza "*inoltre, il presente esame, alla luce dei requisiti posti dall'articolo 52, paragrafo 1, della Carta, verte sul regime specifico di responsabilità dei fornitori di servizi di condivisione di contenuti online, quale introdotto all'articolo 17, paragrafo 4, della direttiva 2019/790, il che non pregiudica un qualsiasi esame che possa riguardare, in una fase successiva, l'esame delle disposizioni adottate dagli Stati membri ai fini del recepimento di tale direttiva o delle misure stabilite da tali fornitori per conformarsi a detto regime*").

In proposito, la CGUE ha evidenziato che gli Stati membri devono pur sempre recepire l'art. 17 CDSMD nel rispetto dei diritti fondamentali ed ha inoltre sottolineato che le autorità e le giurisdizioni degli Stati membri devono vigilare affinché non si agisca sulla base di un'interpretazione della norma che sarebbe in contrasto con tali diritti fondamentali o con gli altri principi generali del diritto dell'Unione, come il principio di proporzionalità (punto 99 della Sentenza: "*Gli Stati membri sono tenuti, in occasione della trasposizione dell'articolo 17 della direttiva 2019/790 nel loro ordinamento interno, a fondarsi su un'interpretazione di tale disposizione atta a garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dalla Carta. Inoltre, in sede di attuazione delle misure di recepimento di tale disposizione, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a detta disposizione, ma anche provvedere a non fondarsi su un'interpretazione di essa che entri in conflitto con i summenzionati diritti fondamentali o con gli altri principi generali del diritto dell'Unione, come il principio di proporzionalità (v., in tal senso, sentenza del 29 gennaio 2008, Promusicae, C-275/06, EU:C:2008:54, punto 68)*".

Per quanto riguarda le conseguenze immediate per gli Stati membri, la Sentenza, pertanto, potrebbe mettere in discussione la validità di alcune parti delle attuazioni nazionali che si basano esclusivamente o prevalentemente su garanzie *ex post* senza limitare anche l'ambito del filtraggio ammissibile, o che contemplano misure di blocco attuate senza contraddittorio o mantenute nelle more di una contestazione.

Per quanto riguarda l'Italia, ad esempio, potrebbe dubitarsi della rispondenza ai principi enunciati nella Sentenza del nuovo art. 102-*decies*, co. 3, l.a., contenuto nel nuovo Titolo II *quater* l.a. rubricato "*Utilizzo di contenuti protetti da parte dei prestatori di servizi di condivisione di contenuti online*", come introdotto dal Decreto di recepimento della direttiva CDSM.

Tale disposizione prevede che i contenuti oggetto di un blocco che venga successivamente contestato dall'autore del relativo caricamento, rimangano non disponibili fino alla risoluzione della controversia ("*Nelle more della decisione sul reclamo, i contenuti in contestazione rimangono disabilitati"*). Questa misura (non prevista, effettivamente, dalla direttiva CDSM) potrebbe essere ritenuta non soddisfacente o non interamente soddisfacente rispetto agli standard elaborati dalla Corte nella Sentenza. Inoltre, alla luce della Sentenza, sembra potersi dire che anche in sede di applicazione giurisprudenziale della nuova disciplina dovrebbe tenersi conto della necessità che siano adottate salvaguardie *ex ante* che limitino l'uso dei filtri automatizzati dei contenuti.

FRANCESCO GROSSI

https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62019CJ0401&from=it

5. Il Governo del Regno Unito annuncia la prossima eliminazione di ogni restrizione all'eccezione di Text and Data Mining (TDM) nei regimi copyright e banche dati per rendere il Regno Unito un "centro mondiale per l'innovazione della IA": il documento pubblicato il 28 giugno 2022 dallo UK Intellectual Property Office

Il 28 giugno 2022, l'*Intellectual Property Office* del Regno Unito ("**IPO**") ha pubblicato un documento in esito ad una consultazione pubblica avviata in data 29 ottobre 2021 (la "**Consultazione Pubblica**") avente ad oggetto le seguenti tre questioni: *1)* se e come modificare il regime del *copyright* in relazione ai contenuti generati dagli elaboratori elettronici (*computer-generated works*); *2)* se e come modificare il regime del c.d. *Text and Data Mining*; *3)* se e come modificare il regime delle invenzioni e dei brevetti in relazione agli *output* di sistemi di intelligenza artificiale.

In esito alla Consultazione Pubblica, la posizione del Governo del Regno Unito, come dichiarata nel citato documento del 28 giugno 2022 (il "**Documento del 28 giugno 2022**") è nel senso di non introdurre allo stato alcuna modifica alle normative del Regno Unito riguardanti le questioni *sub 1)* e *3)*, ma di innovare il regime del c.d. *Text and Data Mining* (questione *sub 2)*), nel senso di eliminare qualsiasi restrizione alle attività di *Text and Data Mining* (di seguito "**TDM**") fondata sul diritto di autore e sul diritto *sui generis* sulle banche dati attraverso l'introduzione di una nuova eccezione a tali diritti che consenta le attività di TDM per qualsiasi finalità. Nel Documento del 28 giugno 2022 viene annunciato che il Governo del Regno Unito individuerà le modifiche legislative più adeguate al fine di conseguire questo obiettivo senza ritardo.

Per comprendere l'importanza della posizione annunciata dal Governo del Regno Unito nel Documento del 28 giugno 2022, si deve, da un lato, ricordare che la questione della regolamentazione delle attività di TDM è stata affrontata dalla direttiva (UE) 2019/790 del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (di seguito la "**direttiva CDSM**" o "**CDSMD**") la quale, agli artt. 3 e 4 prevede alcune eccezioni e limitazioni limitatamente alla finalità di ricerca scientifica e a beneficio soltanto di alcuni soggetti ossia organismi di ricerca e istituti di tutela del patrimonio culturale, con la conseguenza che, fuori da tali ambiti oggettivamente e soggettivamente connotati, le attività di TDM non possono essere legittimamente poste in essere se non sulla base di una autorizzazione dei titolari dei diritti eventualmente incisi dalle medesime attività (sul recepimento in Italia degli artt. 3 e 4 della direttiva CDSM v. la v. la notizia n. **1** nel numero **1/2022** di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf);
dall'altro lato, bisogna ricordare che il Regno Unito aveva già emanato una specifica normativa prima della direttiva CDSM. Si tratta delle norme (ancora in vigore nel Regno Unito in attesa delle modifiche annunciate dal Documento del 28 giugno 2022) contenute nella Sezione 29A del *Copyright, Designs and Patents Act 1988* rubricata "*Copie per analisi di testo e di dati per ricerca non commerciale*" ("*Copies for text and data analysis for non-commercial research*") accessibile su https://www.legislation.gov.uk/ukpga/1988/48/section/29A ("**Normativa UK sul TDM**"), che, con una serie di specificazioni e condizioni, seguono l'impostazione per la quale l'eccezione si applica solo limitatamente alle copie effettuate per finalità di ricerca non commerciale.

Le attività di c.d. *Text and Data Mining* (di seguito "**TDM**") sono definite nel Documento del 28 giugno 2022 come "*l'uso di tecniche computazionali per analizzare grandi quantità di informazioni al fine di individuare modelli, tendenze ed altre informazioni utili*" ("*Text and data mining (TDM) means using computational techniques to analyse large amounts of information to identify patterns, trends and other useful information*."). Nella direttiva CDSM la definizione è la seguente: "*«estrazione di testo e di dati» (text and data mining): qualsiasi tecnica di analisi automatizzata volta ad analizzare testi e dati in formato digitale avente lo scopo di generare informazioni inclusi, a titolo non esaustivo, modelli, tendenze e correlazioni*" (art. 2 CDSMD). Come noto, l'interferenza del TDM con i regimi di esclusiva si pone in relazione alle attività di riproduzione e di estrazione (quest'ultima limitatamente al diritto sui *generis* sulle banche dati), nella misura in cui le medesime attività vengano poste in essere, nel modo previsto dalle normative che le riservono ai titolari dei diritti di esclusiva, nel contesto delle complessive attività di analisi caratterizzanti la nozione di TDM.

Degno di nota è che il Documento del 28 giugno 2022 abbia posto al centro della questione

l'importanza delle attività di TDM per lo sviluppo dei sistemi di intelligenza artificiale, come si vede dallo stesso *wording* del quesito oggetto della Consultazione Pubblica: "*Licenze o eccezioni per il TDM, che è spesso rilevante per l'uso e lo sviluppo dell'IA*" (e v. i punti da 31 a 62 del Documento del 28 giugno 2022), e, ancor più significativamente nel punto 62 del Documento del 28 giugno 2022: "*The Government's ambition is to make the UK a global centre for AI innovation. The new exception will ensure the UK's copyright laws are among the most innovation-friendly in the world […]*".

Le opzioni regolamentari che erano state sottoposte alla Consultazione Pubblica erano le seguenti: opzione 0 = nessun cambiamento rispetto all'assetto normativo esistente, ovvero mantenere l'attuale eccezione limitata alle copie per ricerca non commerciale; opzione 1 = modificare le regole sulle licenze relativamente al TDM; opzione 2 = estendere l'eccezione alla ricerca commerciale; opzione 3 = estendere l'eccezione a qualsiasi scopo, con facoltà di *opt-out* in favore dei titolari dei diritti; opzione 4 = estendere l'eccezione a qualsiasi scopo, senza facoltà di *opt-out* in favore dei titolari dei diritti.

In esito alla Consultazione Pubblica, la posizione del Governo del Regno Unito è stata nel senso dell'opzione 4, ed è stata motivata come segue: "*(59) L'introduzione di una eccezione che si applica al TDM commerciale porterà benefici a un'ampia platea di stakeholders nel Regno Unito, tra cui ricercatori, sviluppatori di IA, piccole imprese, istituzioni di tutela del patrimonio culturale, giornalisti e cittadini impegnati in attività civicamente rilevanti [engaged citizens]. Prodotti e servizi disegnati per i clienti [targeted products and services] gioveranno alle imprese e ai clienti. I risultati della ricerca potranno giovare anche al più ampio pubblico. Ciò potrebbe accadere, ad esempio, supportando la ricerca e l'innovazione nella salute pubblica. Alcuni utilizzano il TDM e l'IA anche nei settori industriali legati alla creatività per comprendere il mercato o creare nuove opere – anche essi vedranno benefici. I benefici ridurranno il tempo necessario per ottenere l'autorizzazione da molteplici titolari di diritti e non saranno dovute commissioni di licenza. Ciò comporterà un'accelerazione del TDM e dello sviluppo della IA. (60) Questi cambiamenti valorizzano al meglio le possibilità conseguenti al Brexit. Esse aiuteranno a rendere il Regno Unito più competitivo come sede di stabilimento per aziende che fanno data mining. (61) I titolari di diritti non potranno più chiedere compensi per licenze rette dalla legge del Regno Unito a titolo di TDM e non potranno negoziare o esercitare facoltà di opt-out per l'eccezione. Il nuovo regime può anche avere conseguenze per coloro che hanno costruito modelli di impresa anche intorno alle licenze di dati. Tuttavia, i titolari di diritti manterranno salvaguardie per proteggere i loro contenuti. La maggiore salvaguardia consisterà nel requisito di un accesso legittimo. Ciò sta a significare che i titolari dei diritti possono scegliere la piattaforma dalla quale essi rendono le loro opere accessibili, e possono chiedere compensi per l'accesso attraverso abbonamento o per singoli accessi. Essi potranno anche adottare misure per assicurare l'integrità e la sicurezza dei loro sistemi. (62) L'ambizione del Governo è di fare del Regno Unito un centro mondiale per l'innovazione dell'IA* […]".

Per quanto riguarda il diritto dell'Unione europea, giova segnalare un recente studio commissionato dalla Commissione Europea, dove si trovano alcune interessanti osservazioni dedicate al TDM, dalle quali emerge la piena consapevolezza dell'importanza delle attività automatizzate di analisi dei dati per lo sviluppo dei sistemi di intelligenza artificiale: European Commission, Directorate-General for Communication, *Study on copyright and new technologies: copyright data management and artificial intelligence*, Publications Office of the European Union, 2022 (https://data.europa.eu./doi/10.2759/570559).

SALVATORE ORLANDO

https://www.gov.uk/government/consultations/artificial-intelligence-and-ip-copyright-and-patents/outcome/artificial-intelligence-and-intellectual-property-copyright-and-patents-government-response-to-consultation#introduction

6. La sentenza della Corte di Giustizia dell'Unione europea del 5 maggio 2022 sull'interpretazione dell'art. 6, par. 1 lett. m) della direttiva 2011/83/UE sui diritti dei consumatori con particolare riferimento agli obblighi informativi del professionista e alla garanzia commerciale del produttore nel contesto del commercio elettronico e delle piattaforme online (caso Victorinox, Causa C-179/21)

Con la sentenza del 5 maggio 2022, nella causa C-179/21 (*Victorinox*), la Corte di giustizia dell'Unione Europea (di seguito anche "**CGUE**") ha precisato l'effettiva portata dell'art. 6, par. 1, lett. m), della direttiva 2011/83/UE sui diritti dei

consumatori, il quale sancisce che il professionista deve fornire al consumatore, in maniera chiara e comprensibile, le informazioni relative all'esistenza e alle condizioni dell'assistenza e dei servizi postvendita nonché delle garanzie commerciali.

Nel caso di specie, la società tedesca *Absoluts - bikes and more- GmbH & Co. KG* poneva in vendita, sulla piattaforma Amazon, il prodotto di un fabbricante svizzero. Nella pagina informativa del prodotto, non vi era alcun riferimento ad una garanzia del produttore ma all'interno della rubrica presente *online*, denominata «*Altre informazioni tecniche*», era inserito un collegamento attraverso cui l'utente poteva accedere a una scheda informativa predisposta dal produttore.

Ritenendo che la società non fornisse informazioni sufficienti sulla garanzia offerta dal produttore, una società concorrente ha proposto, alla luce della disciplina tedesca in materia di concorrenza sleale, un'azione finalizzata a porre fine al commercio *online* di questi prodotti.

La controversia, così, giungeva dinanzi alla Corte federale di giustizia tedesca, la quale si interrogava se ai sensi della direttiva 2011/83/UE sui diritti dei consumatori, un professionista sia tenuto ad informare il consumatore della presenza di una garanzia commerciale del produttore. Inoltre, la Corte tedesca poneva la questione della specifica delimitazione degli obblighi informativi in capo al professionista in simili circostanze di mercato.

Veniva proposto, quindi, rinvio pregiudiziale alla CGUE, la quale, con la sentenza in esame, ha specificato che l'art. 6, par. 1, lett. m), della direttiva sui diritti dei consumatori, deve essere interpretato nel senso che, per quanto riguarda la garanzia commerciale proposta dal produttore, un professionista è tenuto a fornire al consumatore informazioni precontrattuali sulla garanzia commerciale del produttore qualora il consumatore abbia un interesse legittimo a ottenere tali informazioni al fine di potersi vincolare contrattualmente al professionista in maniera consapevole.

Innanzitutto, per quanto riguarda la questione se il professionista sia tenuto a informare il consumatore dell'esistenza di una garanzia commerciale del produttore, la Corte precisa che, qualora l'oggetto del contratto sia un bene prodotto da una persona distinta dal professionista, tale obbligo deve coprire qualsiasi informazione essenziale relativa a tale bene, affinché il consumatore possa decidere se vincolarsi contrattualmente o meno a tale professionista. Secondo la CGUE tali informazioni comprendono le caratteristiche principali del bene nonché la garanzia commerciale proposta dal produttore.

La CGUE, però, correttamente mette in evidenza che al fine di non imporre in capo al professionista un obbligo incondizionato e sproporzionato di fornire siffatte informazioni, in ogni circostanza, esso è tenuto a fornire informazioni precontrattuali al consumatore sulla garanzia commerciale del produttore solo quando il consumatore abbia un interesse legittimo a ottenere tali informazioni.

Bisogna sottolineare che secondo la CGUE, questo obbligo sorge proprio in ragione dell'esistenza di un interesse legittimo del consumatore e non soltanto per il semplice fatto dell'esistenza di tale garanzia. La presenza di questo specifico interesse del consumatore, quindi, si evince dalla circostanza per cui la garanzia commerciale del produttore risulti essere un elemento centrale o determinante dell'offerta. Nello specifico, ciò può rilevare quando il riferimento alla garanzia commerciale diviene uno strumento per aumentare l'attrattività verso i consumatori ed incrementare la competitività rispetto alle offerte dei suoi concorrenti.

Inoltre, per quanto riguarda la seconda questione, ovvero il campo di delimitazione degli obblighi informativi del professionista e, in particolare, in merito alle condizioni relative alla garanzia commerciale del produttore, la CGUE ritiene che il professionista sia tenuto a fornire al consumatore qualsiasi elemento informativo relativo alle condizioni di applicazione ed esecuzione della garanzia commerciale.

Con la sentenza di cui trattasi, la CGUE ha dunque specificato i confini degli obblighi informativi del professionista circa l'esistenza e le condizioni della garanzia commerciale del produttore, nell'ambito del commercio *online* e, più specificatamente, in relazione all'attività di particolari piattaforme digitali come, nel caso di specie, Amazon.

ENZO MARIA INCUTTI

https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62021CJ0179&from=EN

7. Le Linee Guida dell'EDPB n. 5/2022 del 12 maggio 2022 in materia di uso delle tecnologie di riconoscimento facciale con speciale riguardo alle disposizioni della direttiva (UE) 2016/680, c.d. *law enforcement directive*

Il 12 maggio 2022 lo *European Data Protection Board* ("**EDPB"**) ha pubblicato le Linee Guida in materia di uso delle tecnologie di riconoscimento facciale (*facial recognition technologies*, "**FRT"**), deputate a fornire un quadro orientativo per il legislatore europeo e nazionale, le Autorità degli Stati membri e i soggetti privati interessati (di seguito le "**Linee Guida**" o il "**Provvedimento**"). Nello specifico, il Provvedimento si articola in un'analisi delle caratteristiche e dei nodi problematici delle tecnologie in questione e in un'illustrazione della normativa europea applicabile. A ciò si accompagnano tre allegati recanti, rispettivamente, un modello per la descrizione degli scenari, una guida pratica per le Autorità che intendono procurarsi e gestire un sistema FRT e una lista con esempi concreti di impiego delle FRT, allo scopo di agevolare i controlli di necessità e proporzionalità.

In esordio, si rileva il dilagante ricorso alle tecnologie di riconoscimento facciale tanto da parte del settore pubblico quanto dei privati (individui e imprese), dovuto ai forti vantaggi in termini di efficienza e scalabilità. Per contro, si ammonisce che il trattamento automatizzato su larga scala di dati personali e, tra essi, di dati biometrici, è potenzialmente foriero di discriminazioni ed errori di identificazione e rischia di compromettere i diritti fondamentali dei singoli e la stabilità sociale, politica e democratica.

Le FRT sono tecnologie, sovente di intelligenza artificiale, che operano su base probabilistica consentendo il riconoscimento automatico degli individui in base ai connotati dei loro volti. Si tratta di un sottoinsieme della più ampia categoria delle cc.dd. tecnologie biometriche, le quali assommano tutti i processi automatizzati utilizzati per l'identificazione univoca dei soggetti attraverso l'analisi delle caratteristiche fisiche, fisiologiche o comportamentali (impronte digitali, struttura dell'iride, voce, ecc.), definite, a loro volta, "dati biometrici". Il riconoscimento facciale è un processo bifasico: ottenuta un'immagine di un volto umano mediante fotografie o *frame* di video (c.d. "campione biometrico"), le FRT consentono l'estrazione di una rappresentazione digitale (c.d. *template* biometrico); quest'ultimo, asseritamente unico e specifico per ogni persona, viene archiviato in un *database* e, all'occorrenza, comparato con altri modelli. A tali tecnologie si ricorre essenzialmente per finalità di autenticazione o identificazione. Nel primo caso, il sistema confronta il modello estratto in tempo reale da un volto con i *template* biometrici precedentemente memorizzati. Nel secondo, l'esigenza di rintracciare un singolo individuo all'interno di un gruppo richiede l'elaborazione di tanti modelli quanti sono i componenti del gruppo stesso e il successivo confronto con il *template* di riferimento. Gli impieghi concreti sono i più svariati e possono interessare qualunque categoria di soggetti: dall'utente di un servizio o il lavoratore dipendente che necessitino di autenticarsi per accedere, rispettivamente, a un'applicazione o a un luogo di lavoro, fino alla persona da identificare in quanto ricercata o implicata in procedimenti penali o amministrativi. Merita menzione, inoltre, l'attività di categorizzazione biometrica, che ben può basarsi sull'elaborazione di modelli estratti tramite le FRT. In ogni caso, l'EDPB evidenzia che si tratta di stime probabilistiche. Emergono così i due profili pregiudizievoli del riconoscimento facciale: un trattamento avente ad oggetto categorie particolari di dati con un fisiologico coefficiente di fallacia. Ne deriva logicamente che le criticità, massimamente in termini di affidabilità ed efficienza, siano distribuite tanto sul versante dell'*input*, ossia della qualità e la precisione dei campioni biometrici estratti, quanto su quello dell'*output*, ovvero la corrispondenza tra modelli. Il tutto è poi acuito da almeno due fattori: l'oggettiva relatività delle verifiche di accuratezza dei *software* in questione, per la mancanza di criteri univoci, e l'incremento pressoché esponenziale delle conseguenze pregiudizievoli all'aumentare del margine di errore. Su quest'ultimo aspetto, le Linee Guida ricordano come un rapporto dell'Agenzia dell'Unione Europea per i diritti fondamentali del 2019 (https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law) abbia chiarito che, ad esempio, ove si ricorra alle FRT in luoghi aperti al pubblico, l'entità dei campioni estratti fa sì che anche percentuali infinitesimali d'errore si traducano in centinaia di segnalazioni inesatte. Né può ritenersi risolutivo, al riguardo, l'intervento umano, sovente foriero di distorsioni dovute a pregiudizi e idiosincrasie.

Ribadito che l'uso delle FRT ha un sensibile impatto, in via diretta o mediata, sui diritti fondamentali della persona, l'EDPB muove dall'illustrazione del quadro giuridico generale sancito dalla CDFUE (Carta dei diritti fondamentali dell'Unione Europea) e della CEDU (Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali).

Esplicandosi in trattamenti di dati personali, perlopiù appartenenti a categorie particolari, le disposizioni evocate sono anzitutto gli artt. 7 e 8 CDFUE (rispettivamente, sul rispetto della vita privata e familiare e delle comunicazioni e sul diritto alla protezione dei dati personali).

Nondimeno, la mole delle informazioni aggregate che tali sistemi sono in grado di estrarre è tale da incidere anche sulla libertà (o percezione di libertà) di agire delle persone e sull'effettivo esercizio di diritti quali la dignità umana, la libertà di pensiero, coscienza e religione, la libertà di riunirsi pacificamente e di associarsi di cui gli artt. 1, 10, 11 e 12 CDFUE. Ebbene, con l'intesa che qualsiasi trattamento di dati biometrici integra di per sé – e a prescindere dall'esito – una sensibile interferenza con tali posizioni fondamentali, i criteri del bilanciamento sono notoriamente delineati all'art. 52 CDFUE. Qualsiasi limitazione all'esercizio dei diritti e delle libertà fondamentali deve fondarsi su una base giuridica chiara e specifica, salvaguardare l'essenza di diritti e rispettare il principio di proporzionalità, secondo cui le compressioni possono tollerarsi solo se strettamente necessarie ed effettivamente corrispondenti a obiettivi di interesse generale riconosciuti dall'Unione europea o alla necessità di proteggere i diritti e le libertà altrui. In aggiunta, il par. 3 dell'art. 52 e l'art. 53 CDFUE precisano che il significato e la portata dei diritti della medesima Carta, che corrispondono ai diritti garantiti dalla CEDU, devono essere uguali a quelli *ivi* sanciti. Nel caso di specie, il riferimento è all'art. 8 della CEDU, che sancisce il diritto al rispetto della vita privata e familiare.

Come diffusamente rimarcato nel Provvedimento, i rischi connessi alle FRT sono particolarmente elevati nei loro impieghi da parte delle Autorità preposte all'applicazione della legge e in materia di repressione penale e sicurezza pubblica. Per tali ragioni, premesso l'illustrato quadro generale, l'EDPB si concentra sulla direttiva (UE) 2016/680 del 27 aprile 2016, la c.d. *Law Enforcement Directive* ("**LED**"), relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

A venire in rilievo sono anzitutto i principi applicabili al trattamento di dati personali, di cui all'art. 4 LED, e le condizioni di liceità di cui all'art. 8 LED. Quest'ultima disposizione, segnatamente, chiarisce che, per essere lecito, qualsiasi trattamento deve rivelarsi necessario per le finalità di cui all'articolo 1, par. 1 LED e deve basarsi sul diritto dell'Unione o dello Stato membro; e, in quest'ultimo caso, deve essere disciplinato da una legge nazionale che ne specifichi quantomeno gli obiettivi, i dati da trattare e le finalità. In stretto raccordo con tale regime si pone l'art. 10 LED, relativo ai trattamenti di categorie particolari di dati personali, tra cui quelli biometrici. Tali trattamenti sono consentiti solo se strettamente necessari e le relative operazioni devono essere soggette a garanzie adeguate per i diritti e le libertà dell'interessato e autorizzate dal diritto dell'Unione o dello Stato membro, per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o riguardanti dati resi manifestamente pubblici dall'interessato. L'EDPB fornisce preziose indicazioni sul punto. *In primis*, l'art. 10 LED va letto in combinato disposto col Considerando 33 LED, il quale è a sua volta pienamente consonante con gli artt. 52, par. 1 CDFUE e 8, par. 2 CEDU – nonché con la pertinente giurisprudenza europea – nel prescrivere una base giuridica chiara e precisa, allo scopo di assicurarne la prevedibilità da parte degli interessati. Ne deriva un precipuo onere per il legislatore nazionale, che in sede di attuazione della direttiva *in parte qua* non può limitarsi alla mera trasposizione della clausola generale di cui all'art. 10 LED ma dovrà specificare almeno gli obiettivi, i dati personali da trattare, le finalità del trattamento e le procedure per preservare l'integrità e la riservatezza dei dati personali e le procedure per la loro distruzione, premurandosi di consultare previamente l'Autorità garante nazionale, in linea con gli articoli 28, par. 2 e 46, par. 1, lett. *c*). Di poi, le operazioni su categorie particolari di dati sono vincolate a un parametro di stretta necessarietà. Le Linee Guida ricordano che, come statuito dalla giurisprudenza della Corte di Giustizia dell'Unione Europea (Causa C-594/12, punto 52; Causa C-473/12, punto 39 e ulteriore giurisprudenza *ivi* citata), l'avverbio "strettamente" impone un rigore maggiore di quello che assiste il comune test di necessità del trattamento, accostandosi alla indispensabilità secondo criteri oggettivi ben definiti. Infine, il Provvedimento raccomanda particolare cautela allorquando ci si propone di verificare se i dati siano stati resi manifestamente pubblici dall'interessato. In proposito, le Linee Guida osservano che, da un lato, oggetto di pubblicità deve essere il modello biometrico, non essendo sufficiente la divulgazione di fotografie o raffigurazioni del volto; dall'altro, deve tenersi presente che dalla mera condivisione di immagini su *social network* o piattaforme online da parte dell'interessato non è dato inferire meccanicamente un intento di rendere manifestamente pubblici i propri dati.

Proseguendo, le Linee Guida ricordano che l'art. 11, par. 1 LED sul processo decisionale automatizzato relativo alle persone fisiche pone un generale divieto delle decisioni basate unicamente sul trattamento automatizzato, compresa la

profilazione, ove producano un effetto giuridico negativo sull'interessato o lo danneggino in modo significativo. Sono ammesse deroghe solo a condizione che tali operazioni siano autorizzate dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare e prevedano garanzie adeguate per i diritti e le libertà dell'interessato, tra cui almeno il diritto di ottenere l'intervento umano. Un regime ancor più restrittivo è riservato dal par. 2 alle decisioni basate sulle categorie particolari di dati di cui all'art. 10 LED: esse sono ammissibili solo se esistono misure idonee a salvaguardare i diritti e le libertà dell'interessato e gli interessi legittimi della persona fisica coinvolta. In ogni caso, osserva l'EDPB nel Provvedimento, l'impiego di FRT che si esplichi in profilazioni discriminatorie è sempre vietato, senza deroga alcuna, ai sensi dell'art. 10, par. 3 LED. Inoltre, le verifiche di necessità e proporzionalità degli usi delle FRT devono essere condotte anche in relazione alle categorie dei soggetti interessati. Al riguardo, importanti indicazioni sono offerte dalla tassonomia – meramente esemplificativa – illustrata all'art. 6 LED. Converrà, sul punto, rimarcare che le norme della LED vanno lette in conformità ai canoni del bilanciamento enucleati al menzionato art. 52 CDFUE, di cui gli atti legislativi europei e nazionali devono assicurare la piena effettività.

Soddisfatte le stringenti condizioni testé illustrate, l'EDPB pone particolare enfasi sulla disamina dei diritti che la LED conferisce agli interessati, in perfetta consonanza col GDPR. L'impiego di tecnologie di riconoscimento facciale pone anzitutto difficoltà nel garantire una concreta consapevolezza delle persone circa lo svolgimento di trattamenti sui propri dati biometrici. In quest'ottica, l'art. 13, par. 1 LED individua un nucleo minimo di informazioni generali da mettere a disposizione del pubblico, attinenti a: l'identità e i dati di contatto del titolare del trattamento; i dati di contatto del responsabile della protezione dei dati, se del caso; le finalità del trattamento cui sono destinati i dati personali; il diritto di proporre reclamo a un'autorità di controllo e i dati di contatto di detta autorità; l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati e la rettifica o la cancellazione dei dati personali e la limitazione del trattamento dei dati personali che lo riguardano. In aggiunta, il par. 2 del medesimo articolo prescrive obblighi informativi supplementari, da assolvere in casi specifici (tra cui certamente gli usi di FRT) nei confronti dei soggetti specificamente interessati: la base giuridica del trattamento; il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; se del caso, le categorie di destinatari dei dati personali, anche in paesi terzi o in seno a organizzazioni internazionali; se necessario, ulteriori informazioni, in particolare nel caso in cui i dati personali siano raccolti all'insaputa dell'interessato. Cosa debba intendersi per "casi specifici" non è specificato nel testo legislativo. L'incertezza interpretativa è in parte colmata dalle Linee Guida, che enucleano alcuni indici sintomatici quali l'estrazione di dati all'insaputa dell'interessato, o il trattamento ulteriore degli stessi in seno a procedure di cooperazione internazionale in materia penale o nell'ambito di operazioni segrete in base alla legislazione nazionale. Un'ulteriore indicazione è fornita dal Considerando 38 LED, che assegna rilievo centrale all'informazione nelle ipotesi di decisioni basate esclusivamente su trattamenti automatizzati che incidano negativamente o, comunque, significativamente sulla persona dell'interessato. In ogni caso, in ossequio al principio di minimizzazione di cui all'art. 4, par. 1, lett. *a*) LED, qualsiasi campione biometrico che esuli dallo scopo del trattamento (o dalla materia dell'indagine) va rimosso o reso anonimo in modo irreversibile da parte delle Autorità.

Funzionale alla soddisfazione dell'interesse cognitivo dei soggetti interessati è anche il diritto di accesso di cui all'art. 14 LED, che si articola nella facoltà di ottenere la conferma dei trattamenti in essere sui propri dati personali e, in caso di risposta positiva, l'accesso a tali dati e a una serie di informazioni aggiuntive.

Poiché uno dei profili più preoccupanti dei sistemi di riconoscimento facciale è la loro operatività su base probabilistica, le Linee Guida opportunamente sottolineano l'impennarsi dei rischi laddove le FRT siano impiegate per finalità di identificazione, con conseguente raccolta di dati biometrici su larga scala ed eventuale archiviazione in banche dati condivise tra più Autorità. Ebbene, come contropartita compensativa dei possibili deficit di accuratezza, sono conferiti dall'art. 16 LED il diritto di rettifica dei dati inesatti e di cancellazione (senza ingiustificato ritardo) di quelli estratti in base a trattamenti illeciti. In relazione ai limiti che incontrano le verifiche di accuratezza dei *software* in questione, per la mancanza di criteri univoci, e nei casi in cui tali accertamenti non siano obiettivamente possibili, all'obbligo di cancellazione tiene luogo quello di limitazione del trattamento secondo i parametri del Considerando 47 LED. Orbene, le istanze protettive suggellate nei diritti summenzionati sono antitetiche ad alcune esigenze sottese all'uso di FRT per fini di applicazione della legge, che verrebbero

concretamente vanificate se gli interessati venissero informati o ottenessero l'accesso ai dati. La misura del bilanciamento è variamente fissata dagli artt. 13, par. 3, 15, 16, par. 4 LED ove concorrano interessi di rilievo primario quali la non compromissione di indagini, inchieste, procedimenti ufficiali o giudiziari, ovvero della prevenzione, dell'indagine, dell'accertamento, del perseguimento di reati o dell'esecuzione di sanzioni penali, la protezione della sicurezza pubblica, della sicurezza nazionale, dei diritti e delle libertà di terzi. In tali ipotesi di legittima compressione dei diritti assegnati dal Capo III della LED, gli interessati beneficiano del presidio *ex* art. 17 LED, che impone agli Stati membri di adottare misure che consentano l'esercizio "mediato" di tali diritti per il tramite delle Autorità Garanti nazionali.

Accanto alle posizioni soggettive azionabili, il quadro delle tutele per i soggetti è completato da una serie di obblighi imposti ai titolari e ai responsabili del trattamento. In estrema sintesi: la protezione dei dati fin dalla progettazione e per impostazione predefinita, volto a garantire le tecnologie incorporino adeguate salvaguardie fin dall'origine (art. 20 LED); la tenuta di registri di sistema relativi almeno alle operazioni di raccolta, modifica, consultazione, divulgazione, compresi i trasferimenti, combinazione e cancellazione, che fungono da punto di riferimento per i controlli, sia interne che esterni (art. 25 LED); l'obbligo di una previa valutazione dell'impatto sulla protezione dei dati personali (DPIA), di cui l'EDPB incoraggia la pubblicazione, in particolare laddove l'impiego di nuove tecnologie può comportare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 27 LED); la consultazione dell'Autorità di controllo (ex art. 28 LED) prima della distribuzione del sistema FRT; l'adozione e il mantenimento di misure per garantire un livello di sicurezza dei trattamenti adeguato al rischio (art. 29 LED).

Andando a concludere, l'EDPB ribadisce nelle Linee Guida che l'uso delle tecnologie di riconoscimento facciale implica fatalmente il trattamento di cospicue quantità di dati personali, compresi quelli appartenenti a categorie particolari come i dati biometrici. Quest'ultimi, per essere collegati in modo permanente e irrevocabile all'identità di una persona, rendono tali operazioni fortemente stridenti con una serie di diritti e libertà fondamentali, vieppiù se condotte nel settore dell'applicazione della legge e della giustizia penale. Il bilanciamento tra le istanze in conflitto deve condursi nel pedissequo rispetto dei principi di legalità, necessità e proporzionalità e deve essere condotto caso per caso all'esito di una ragionevole ponderazione degli interessi in gioco. In alcuni casi, l'impiego di sistemi FRT produce risultati assolutamente intollerabili, di cui l'EDPB e il Garante europeo dei dati personali (lo *European Data Protection Supervisor*, "**EDPS**") hanno già suggerito il radicale divieto nel parere congiunto n. 5/2021 del 18 giugno 2021 (https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_it.pdf) e nel pronunciamento congiunto del 21 giugno 2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate in materia di intelligenza artificiale (https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en, su quest'ultimo v. la notizia n. **3** nel numero **3/2021** di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2021/08/Osservatorio.pdf). In particolare, si fa riferimento alla identificazione biometrica a distanza di persone in spazi accessibili al pubblico, alla categorizzazione biometrica, ai sistemi di riconoscimento delle emozioni e, più in generale, al trattamento per fini di applicazione della legge basato su una banca dati che contenga informazioni raccolte su scala di massa e in modo indiscriminato, ad esempio attingendo dalle immagini rese disponibili sui social network.

VALENTINO RAVAGNANI

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_it

8. Il Parere della Banca Centrale Europea del 29 dicembre 2021 sulla proposta di regolamento sull'intelligenza artificiale.

Il 29 dicembre 2021 la Banca Centrale Europea (di seguito anche la "**Banca**" o la "**BCE**") ha reso un parere riguardo alla proposta di regolamento sull'intelligenza artificiale del 21 aprile 2021 (da ora anche l'"***Artificial Intelligence Act***" o "**AIA**") presentata dalla Commissione (su cui v. notizia n. **1** nel numero **2/2021** di questa Rubrica: *http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio-1.pdf*). A tale parere (CON/2021/40) (2022/C 115/05) pubblicato nella Gazzetta Ufficiale dell'11 marzo 2022 (di seguito solo il "**Parere**"), si accompagna un "documento tecnico" contenente dettagliate proposte di modifica dell'AIA. Nel Parere, la BCE presenta delle interessanti riflessioni su alcuni aspetti dell'*Artificial Intelligence Act* che, non a

caso, hanno richiamato l'attenzione degli studiosi e sono stati oggetto di (ulteriori) proposte di modifica del testo originale dell'AIA da parte del Consiglio dell'UE e del Parlamento europeo.

Il parere si articola in tre sezioni: 1) osservazioni di carattere generale; 2) il ruolo della BCE ai sensi della proposta di regolamento; 3) classificazione dei sistemi di IA.

1) Osservazioni di carattere generale.

La BCE, innanzitutto, accoglie favorevolmente il tentativo della proposta di dettare norme uniformi per "*lo sviluppo, la commercializzazione e l'uso di un'intelligenza artificiale … affidabile*" che hanno il pregio di migliorare il mercato interno (par. 1.1 del Parere). La proposta in commento, peraltro, è rilevante anche in virtù della crescente importanza dell'intelligenza artificiale ("**IA**") nel settore bancario. Tanto che la BCE suggerisce l'istituzione di un'autorità indipendente per l'intelligenza artificiale a livello europeo che garantisca un'attuazione armonizzata della disciplina in commento (par. 1.2 del Parere).

Dalla lettura della proposta di regolamento (in particolare gli artt. 9, par. 9, 18, par. 2, 20, par. 2 e 29, par. 5 – non oggetto delle recenti proposte di modifica del Parlamento europeo e del Consiglio), inoltre, la BCE rileva che sono state integrate alcune norme della direttiva 2013/36/UE del 26 giugno 2013 sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE ("Capital Requirements Directive", c.d. CRD) intervenendo sulla *governance* bancaria (par. 1.3 del Parere). Si tratta, ancora una volta, di una modifica valutata positivamente dalla BCE e che consente di migliorare l'organicità della disciplina di settore. Considerata la delicatezza della materia, tuttavia, la Banca rileva che sarebbe opportuno non intaccare gli obblighi prudenziali degli enti creditizi, come sembrerebbero invece prospettare le citate norme della Proposta di AIA. Il Parere reputa, pertanto, necessario che siano forniti chiarimenti riguardo ai "*requisiti applicabili e alle autorità competenti per quanto riguarda l'esternalizzazione da parte degli enti creditizi utenti di sistemi di IA ad alto rischio*" (par. 1.4 e 1.5 del Parere).

Allo stesso modo, nel Parere si osserva che la proposta di AIA dovrebbe chiarire il ruolo assegnato alla BCE per quanto riguarda i) la vigilanza prudenziale, del mercato e la valutazione di conformità dei sistemi di IA; ii) l'influenza dell'AIA sull'assolvimento dei compiti istituzionali della BCE (par. 1.6 del Parere).

2) Il ruolo della BCE ai sensi della proposta di regolamento.

i) In merito alla vigilanza del mercato, la Banca desume che non può essere l'autorità incaricata di tale compito cui si riferisce l'AIA. La proposta di *Artificial Intelligence Act*, nell'individuare l'autorità di vigilanza del mercato rinvia al Regolamento (UE) 2019/1020, istitutivo del Meccanismo di Vigilanza Unico (c.d. MVU), che designa quale authority competente quella di ciascuno Stato membro all'uopo designata (par. 2.1.5 del Parere).

Sennonché, l'art. 63, par. 4 della proposta di AIA (anche a seguito delle proposte recenti di modifica del Parlamento europeo e del Consiglio) prevede che l'autorità di vigilanza del mercato sia quella responsabile della vigilanza finanziaria sugli enti creditizi, che ben può essere la BCE. Siccome, però, la vigilanza del mercato mira a tutelare gli interessi dei singoli e non la solidità e sicurezza degli istituti di credito, compito spettante alla BCE, quest'ultima "*evince che il legislatore dell'Unione non propone che la BCE agisca come autorità di vigilanza del mercato in relazione agli enti creditizi sottoposti alla sua vigilanza*".

S'impone, allora, un miglior coordinamento tra la proposta in commento e il Regolamento (UE) 2019/1020. "*Il testo della proposta di regolamento dovrebbe chiarire in modo inequivocabile che la BCE non è designata come autorità di vigilanza del mercato né incaricata di compiti di vigilanza del mercato*" (parr. 2.1.3 - 2.1.6 del Parere).

Per di più, la Banca rileva che le norme dell'AIA riguardanti la vigilanza del mercato non affrontano adeguatamente il caso in cui un sistema di IA sia messo in servizio da un istituto di credito per uso proprio. In tal caso, laddove l'autorità di vigilanza designata ai sensi dell'AIA ritiri dal mercato un sistema di IA, l'ente creditizio che ne faccia un uso proprio ai sensi della proposta di regolamento non sarebbe obbligato a cessarne l'utilizzazione. Pure in questo caso, dunque, è opportuno un intervento chiarificatore del legislatore europeo che specifichi "*quali misure restrittive e quali relativi poteri delle autorità competenti debbano applicarsi a situazioni di uso proprio*" (par. 2.1.8).

ii) In merito alla valutazione della conformità dei sistemi di IA, gli artt. 19, par. 2 (di cui il Parlamento europeo ha proposto l'eliminazione dal testo dell'AIA) e 43, par. 2 (non intaccato dalle proposte recenti di modifica) della proposta di *Artificial Intelligence Act* stabiliscono che i sistemi di IA ad alto rischio immessi sul mercato o messi in servizio dagli enti creditizi e destinati ad essere utilizzati per valutare l'affidabilità creditizia degli individui o stabilire il loro merito creditizio

debbano superare una valutazione di conformità nell'ambito del processo condotto dalla BCE di revisione e valutazione prudenziale di cui agli articoli da 97 a 101 direttiva 2013/36/UE (c.d. SREP) (par. 2.2.1).

Nel Parere, la Banca si dichiara disponibile ad assolvere tale compito, ma, al contempo, invita il legislatore europeo a prevedere che siano designate delle autorità nazionali che valutino la conformità dei sistemi di IA rispetto alle norme sulla salute, sicurezza e diritti fondamentali dell'UE (par. 2.2.2 del Parere).

Nondimeno, la BCE invita (nuovamente) a riflettere sull'istituzione di un'autorità europea per l'IA che avrebbe il pregio di garantire un'applicazione uniforme dell'AIA (par. 2.2.3).

Il Parere, inoltre, evidenzia che la valutazione di conformità dei sistemi di IA ad alto rischio destinati ad essere utilizzati per valutare l'affidabilità creditizia degli individui o stabilire il loro merito creditizio è intesa dall'*Artificial Intelligence Act* come un controllo interno al fornitore - qui l'istituto di credito - svolto *ex ante* rispetto all'immissione sul mercato o alla messa in servizio da parte dagli enti creditizi. Nella misura in cui, però, tale valutazione debba essere svolta nell'ambito dello SREP, la Banca consiglia una modifica della proposta di AIA per precisare la natura di controllo *ex post* della valutazione di conformità.

La BCE, infine, similmente a quanto osservato da diversi studiosi, sottolinea la scarsa chiarezza dei requisiti di un sistema di IA per essere classificato come ad alto rischio (par. 2.2.4 del Parere).

iii) Riguardo alle competenze della BCE in materia di vigilanza prudenziale, la Banca precisa di poter svolgere le funzioni assegnate dall'AIA ad un'autorità di vigilanza nei limiti "*dei compiti ad essa attribuiti dal regolamento sull'MVU*". Se ne desume che le sue competenze sono limitate. Di conseguenza, per evitare che il richiamo operato dall'AIA alle funzioni dell'autorità di vigilanza sia inoperante, il parere suggerisce che nella proposta di regolamento si faccia riferimento alle autorità di vigilanza per come individuate dai singoli atti dell'Unione Europea. In tal modo, il richiamo alle autorità di vigilanza non sarebbe limitato alla BCE (par. 2.3).

iv) Il parere, infine, precisa che la BCE e le Banche centrali nazionali possono agire loro stesse come fornitori o utenti di sistemi di IA.

Ora, laddove le istituzioni dell'UE siano assoggettate alla disciplina dell'AIA, la proposta di regolamento affida al Garante europeo della protezione dei dati (GEPD, o EDPS nell'acronimo inglese) il ruolo di autorità di vigilanza. Dal canto suo, il parere precisa che le Banche centrali nazionali, invece, potrebbero essere assoggettate al controllo dei rispettivi garanti nazionali della protezione dei dati. In ogni caso, il Parere sottolinea la necessità che la BCE e le Banche centrali nazionali possano svolgere i propri compiti "*in modo indipendente*" (par. 2.4 del Parere).

3) Classificazione dei sistemi di IA.

Il Parere rileva che l'Artificial Intelligence Act è costruito sul c.d. *risk based approach*, ossia prevede una serie di obblighi del fornitore e tutele dell'utente "proporzionalmente" crescenti in funzione della maggiore rischiosità del sistema di IA.

Il provvedimento in esame, inoltre, rileva che la definizione di sistema di IA ad alto rischio è tratteggiata in termini tanto ampi da ricomprendervi molte attività svolte dagli enti creditizi, tra cui quelle di *credit scoring*, finendo così per gravare tali soggetti di una serie di obblighi, anche se il sistema di IA, di per sé, non presenta rischi elevati (par. 3.1). Tale circostanza, oltretutto, contrasta con la suddetta logica proporzionale dell'*Artificial Intelligence Act*. La BCE, quindi, suggerisce di escludere i sistemi di *credit scoring* da quelli ad alto rischio purché "*l'impatto di tali approcci sulla valutazione dell'affidabilità creditizia o del merito di credito delle persone fisiche sia minimo*" (par. 3.2 del Parere).

La Banca auspica che i criteri delineati dall'AIA per la classificazione di un sistema di IA come ad alto rischio entrino in vigore solo dopo che la Commissione abbia adottato le specifiche comuni di cui all'art 41, par. 1 della proposta di regolamento. Nondimeno, sarebbe preferibile che la BCE fosse consultata prima dell'adozione di tali specifiche riguardanti sistemi di *credit scoring* per assicurare l'organicità e il coordinamento delle disposizioni dell'AIA. Il Parere prosegue rappresentando che le specifiche, da un lato, dovrebbero stabilire quando un sistema di IA ad alto rischio in ambito creditizio sia conforme ai requisiti della proposta di regolamento. Dall'altro, dovrebbero permettere di comprendere quando i sistemi di IA possano essere definiti come "*«messi in servizio da fornitori di piccole dimensioni per uso proprio» e rientrare pertanto nell'ambito di applicazione dell'eccezione alla qualifica di sistema di IA ad alto rischio*" di cui al punto 5, let. b) dell'Allegato III alla proposta di regolamento (par. 3.3 del Parere).

Su tale ultimo punto, occorre precisare che il parere della BCE è precedente ad alcune proposte di modifica del testo dell'*Artificial Intelligence Act* formulate dal Parlamento europeo, che ha ipotizzato proprio di eliminare l'eccezione di cui al punto 5, lett. b) dell'Allegato III dell'AIA. Le osservazioni

del Parere, dunque, potrebbero essere superate qualora fossero approvate le proposte di modifica del Parlamento europeo.

Il Parere, infine, esprime apprezzamento per la possibilità offerta dall'art. 7, par. 1 AIA di aggiornare l'elenco dei sistemi di IA ritenuti ad alto rischio, attività a cui la BCE si dice "*pronta a cooperare*". Anche la menzionata norma è stata oggetto di proposte di modifica del Parlamento europeo, ma le osservazioni della BCE sono tuttora valide.

La possibilità di modifica dell'elenco si rivela assai utile poiché, da un lato, come rilevato anche dalla dottrina, l'Allegato III comprende fattispecie eterogenee, che forse richiederebbero un'armonizzazione: sono accomunati sistemi di IA molto complessi con altri meno o addirittura dal carattere compilativo.

Dall'altro lato, l'intelligenza artificiale è caratterizzata da una rapida evoluzione che rende l'elenco di cui all'Allegato III soggetto a obsolescenza e incompletezza.

A tal proposito, il Parere evidenzia che gli enti creditizi stanno sviluppando o "*valutando lo sviluppo e l'utilizzo della modellizzazione dei dati di IA che collegano vendite, transazioni e dati sulle prestazioni … Analogamente, i sistemi di IA potrebbero essere utilizzati nel monitoraggio in tempo reale dei pagamenti, o nella profilazione dei clienti o delle operazioni, a fini di lotta al riciclaggio di denaro e al finanziamento del terrorismo*" (par. 3.4 del Parere). E potrebbe essere opportuno includere tali sistemi di IA nell'Allegato III dell'AIA.

In conclusione, la BCE esprime un parere sostanzialmente positivo sulla proposta di regolamento di AIA, ma non manca di formulare alcuni rilievi e altrettante proposte di modifica.

EMANUELE STABILE

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52021AB0040

9. Il Regolamento di Banca d'Italia del 22 marzo 2022 sul trattamento dei dati personali effettuato nell'ambito della sua gestione degli esposti

Il 22 marzo 2022 la Banca d'Italia (di seguito anche la "**Banca**" o "**BdI**") ha adottato con la Delibera n. 112/2022 un regolamento disciplinante il trattamento dei dati personali effettuato dalla stessa BdI nella gestione degli esposti riguardanti la trasparenza delle condizioni contrattuali, la correttezza dei rapporti tra intermediari e clienti e i diritti e gli obblighi delle parti nella prestazione dei servizi di pagamento (da ora anche il "**Regolamento**"). Esso integra un regolamento del 6 novembre 2015 della stessa BdI sull'individuazione dei dati sensibili e giudiziari e delle operazioni eseguibili sugli stessi.

Preliminarmente, bisogna rilevare che l'adozione del provvedimento in parola è stata preceduta da un parere favorevole del Garante per la protezione dei dati personali (di seguito anche il "**Garante**") reso il 24 febbraio 2022. Per quanto qui interessa, il Garante apprezza che nel Regolamento:

1) facendo buon governo dei principi di liceità, correttezza e trasparenza, siano state precisate "*tipologie di dati trattati, categorie di interessati, operazioni eseguibili e modalità del trattamento*" al fine di meglio distinguere i vari trattamenti dei dati effettuati;
2) siano state previste misure specifiche a tutela degli interessati, tra cui l'avviso che il trattamento è in corso, delle sue caratteristiche e delle garanzie assicurate dalla BdI;
3) si escluda la trasmissione di dati ed elaborazioni a soggetti esterni alla BdI;
4) sia individuato un periodo di conservazione dei dati di dieci anni, fermi i diritti ex art. 21 GDPR;
5) si introduca un monitoraggio e una maggiore trasparenza delle tecniche di *machine learning*.

Secondo il Garante, il Regolamento rispetta sia "*i principi di accountability e di privacy by design e by default*" delineati dagli artt. 5, par. 2, 24 e 25 del GDPR, sia alcune norme, tra cui l'art. 14, della proposta di Regolamento sull'intelligenza artificiale (c.d. "*Artificial Intelligence Act*") presentato dalla Commissione il 21 aprile 2021. Occorre rilevare, che diverse disposizioni dell'*Artificial Intelligence Act* hanno subito proposte di modifica successivamente all'emanazione del Parere. Condivisibilmente, inoltre, il Garante prescrive una continua analisi dei rischi connessi al trattamento e l'aggiornamento della relativa valutazione d'impatto.

Venendo all'analisi del Regolamento bisogna, innanzitutto, premettere che la Delibera, cui è allegato il provvedimento in esame, nella parte motivazionale evidenzia che la gestione degli esposti "*rappresenta un compito di interesse pubblico*" della Banca.

Per quanto qui interessa, la Delibera consta di soli tre articoli e all'art. 1 definisce l'oggetto del Regolamento, ossia l'identificazione delle

"*tipologie di dati personali trattati nonché le operazioni eseguibili e le misure di sicurezza adottate dalla Banca d'Italia nell'ambito della gestione degli esposti*".

L'art. 2 si limita a stabilire che nel Regolamento sono dettate disposizioni specifiche sulle finalità e modalità del trattamento dei dati.

L'art. 3, infine, per quanto non previsto dal Regolamento rinvia a quello del 6 novembre 2015 sopra detto.

Ebbene, la lett. a) del Regolamento (diviso in lettere, non articoli) rubricata "*attività di gestione degli esposti*", in primo luogo, precisa che diversi soggetti, a vario titolo, possono inviare degli esposti alla Banca riguardo alla trasparenza delle condizioni contrattuali, la correttezza dei rapporti tra intermediari vigilati e clientela e i diritti e gli obblighi delle parti nella prestazione di servizi di pagamento.

Ciò determina che la Banca d'Italia svolga, sostanzialmente, un duplice trattamento dei dati: i) nella gestione degli esposti; ii) nell'uso delle informazioni acquisite tramite "*strumenti di intelligenza artificiale*" (da ora anche "**IA**").

Riguardo al trattamento sub i), il Regolamento precisa che i dati di cui la Banca viene a conoscenza con gli esposti non sono predeterminabili ex ante, ma normalmente contengono elementi che consentono l'identificazione dell'esponente ed, eventualmente, della persona che effettua la segnalazione per suo conto, nonché i recapiti a cui indirizzare le comunicazioni successive alla presentazione dell'esposto. La segnalazione contiene altresì una rappresentazione dei fatti all'origine dell'esposto.

Laddove la questione segnalata sia effettivamente di competenza della Banca, e non debba essere reindirizzata ad altra Autorità di supervisione, inoltre, l'esposto implica pure l'interpello dell'intermediario vigilato cui afferisce la segnalazione e l'invio ad esso di una copia della stessa. Gli intermediari, inoltre, possono fornire "*informazioni e documenti*" a supporto delle loro tesi difensive che ben possono rivelare altri dati, come: rapporti bancari e finanziari, categorie particolari di dati personali e dati relativi a condanne penali e reati riguardanti tanto l'esponente quanto soggetti terzi.

Riguardo al trattamento dei dati che la Banca svolge sub ii), il Regolamento stabilisce che le segnalazioni, sia cartacee sia digitali tramite apposito portale della Banca, sono spesso composte da voluminosi documenti e l'utilizzo di strumenti di IA è necessario per "*estrarre concetti e ricorrenze e … connettere informazioni*". Tale trattamento avviene tramite un motore di ricerca *full text* che, accedendo a tutti i documenti, individua le similarità tra di essi. Nondimeno, tramite tecniche di analisi e algoritmi di *machine learning* in grado di apprendere le logiche di analisi e ricerca da un insieme di dati, c.d. *training dataset*, si estraggono gli elementi e i documenti più rilevanti fino ad aggregare i dati in cluster a cui si assegnano dei tag esemplificativi che consentono di desumere informazioni ulteriori rispetto a quelle originali. Il Regolamento precisa che non viene assolutamente effettuata una clusterizzazione degli esponenti e/o dei soggetti terzi sulla base dei dati personali. L'uso dell'IA non è nemmeno strumentale ad una profilazione o predizione di comportamenti, ma solo ad analizzare l'evoluzione di un fenomeno. Non a caso, il Regolamento precisa che "*dai risultati dell'analisi non derivano conseguenze sanzionatorie o decisioni automatiche su persone fisiche … tali decisioni rientrano nell'esercizio discrezionale delle funzioni di vigilanza*".

La lett. b) stabilisce che, nel rispetto dei principi di liceità e limitazione delle finalità del trattamento, i dati acquisiti dalla Banca tramite gli esposti sono gestiti nel rispetto della normativa sul trattamento dei dati personali e, salvo esigenze di pubblico interesse, conservati per il tempo strettamente necessario al loro trattamento. Il tempo di conservazione limite è stabilito nel Massimario di scarto della Banca per le attività di gestione degli esposti e non può essere superiore a dieci anni per l'utilizzo delle informazioni acquisite tramite le segnalazioni.

Analogamente alla predetta Delibera, la lett. c) del Regolamento ricorda che la gestione degli esposti risponde a un'esigenza di pubblico interesse, ossia il controllo sugli intermediari vigilati.

La lett. d) individua la base giuridica del trattamento richiamando il D. Lgs. 385/1993, il D. Lgs. 58/1998, la L. n. 262/2005, il D. Lgs. 11/2010, la delibera CICR 286/2003 nonché il provvedimento della stessa Banca d'Italia del 29 luglio 2009.

La lett. e), similmente alla lett. a), definisce le tipologie di dati trattati che sono "*dati personali idonei a identificare in modo diretto o indiretto una persona fisica; categorie particolari di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché dati relativi alla salute o alla vita sessuale o all'orientamento sessuale di una persona fisica; dati personali relativi a condanne penali e reati o a connesse misure di sicurezza*".

Ai sensi della lett. f), i soggetti interessati al trattamento dei dati sono le persone fisiche esponenti o soggetti terzi, individuati nelle "*persone*

fisiche che, quali mittenti, agiscono per conto dell'esponente; persone fisiche legate, per rapporti di parentela, amicizia, professionali o di altra natura, agli esponenti e coinvolte a vario titolo nella vicenda; persone fisiche che svolgono funzione di direzione, amministrazione e controllo o che operano attraverso rapporto di lavoro o mandato con l'intermediario coinvolto, ...; consulenti finanziari o intermediari del credito".

La lett. g) del provvedimento in esame, richiamando la lett. a), descrive le operazioni eseguibili sugli esposti che includono:

i) la "*raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento, estrazione, consultazione, uso, raffronto, interconnessione, limitazione, cancellazione dell'esposto e dei dati ivi contenuti, condotte con e senza l'ausilio di sistemi di IA e tecnologie innovative*". Si tratta della gestione degli esposti che include pure la comunicazione all'esponente dell'avvenuta ricezione della segnalazione, l'analisi della risposta dell'intermediario, lo scambio di informazioni con altri uffici di Banca d'Italia e la comunicazione dell'esposto ad alcune autorità pubbliche elencate nel Regolamento;

ii) l'analisi della segnalazione attraverso la ricerca di precedenti;

iii) la decisione tra adottare provvedimenti o archiviare l'esposto.

Tra le misure tecniche e organizzative a tutela degli interessati, la lett. h) del Regolamento precisa che sono state adottate una serie di precauzioni per evitare eventi malevoli, come: la predisposizione e costante rivisitazione di , interne sulla protezione dei dati; misure per la continuità operativa e la gestione degli incidenti di sicurezza.

In particolare, è stato previsto: l'accesso alle informazioni ai soli dipendenti abilitati muniti di account e password; l'elaborazione di *backup* periodici; misure di protezione delle apparecchiature informatiche; il riaddestramento degli algoritmi di *machine learning*, per evitare l'obsolescenza delle relazioni apprese dal modello, è eseguito da data scientists. Riguardo a tale ultimo aspetto, il Regolamento rappresenta che la documentazione comprovante il perfezionamento dell'algoritmo è conservata solo per fini di *versioning* del modello e di monitoraggio del suo sviluppo.

La lett. i), infine, precisa che l'informativa agli interessati sul trattamento dei dati e il provvedimento in esame sono pubblicati sul sito web della BdI e che gli interessati possono comunque esercitare tutti i diritti ex artt. 15 - 22 GDPR.

EMANUELE STABILE

https://www.bancaditalia.it/media/notizia/regolamento-sul-trattamento-dei-dati-personali-nella-gestione-degli-esposti/?dotcache=refresh&dotcache=refresh

10. La dichiarazione del Presidente del Garante Privacy italiano sui 'neurorights' del 30 maggio 2022: l'auspicio alla definizione di uno "statuto giuridico ed etico dei neurodiritti"

Lo sviluppo tecnologico nel campo degli studi sul cervello umano – neuroscienze - ha determinato negli ultimi anni un'attenzione sempre crescente da parte del giurista per le notevoli questioni che si pongono in conseguenza dell'utilizzo di devices particolarmente sofisticati. Si tratta, più in particolare, delle c.d. neurotecnologie, ovvero di un complesso eterogeneo di metodi e strumenti tecnologici che consentono di creare un percorso di comunicazione diretto con il cervello umano attraverso la lettura e decodifica del segnale celebrale (tecnologie c.d. "brain reading"). Tali dispositivi (è il caso della Risonanza magnetica funzionale_fMR o delle varie interfacce cervello-computer ovvero Brain computer interface_BCI) sono attualmente impiegati principalmente in ambito clinico per la diagnosi ed il trattamento di patologie gravemente invalidanti e neurodegenerative. Si tratta delle più recenti applicazioni dell'intelligenza artificiale in ambito neuroscientifico e neurotecnologico che consentono di incidere sulla parte meno esplorata della persona umana, ovvero il cervello. Ciò induce a riflettere sulle possibili esigenze di tutela della persona umana in ambiente tecnologico al fine di evitare situazioni di vulnerabilità di soggetti - persone con disabilità e/o consumatori - per i quali non vi sarebbe alcuna tutela giuridica rispetto ad un utilizzo distorto delle interfacce di collegamento tra il cervello e l'ambiente esterno. I profili di rilevanza etica e giuridica sono molteplici e non possono che riguardare anche questioni di data protection. In proposito è intervenuto con particolare attenzione e in diverse occasioni il Presidente dell'Autorità Garante per la protezione dei dati personali, Prof. Pasquale Stanzione, il quale ha sottolineato la necessità che l'utilizzo delle neurotecnologie sia

adeguatamente regolamentato, anche attraverso la tutela di nuovi diritti fondamentali, c.d. neurodiritti (da ultimo con una dichiarazione sul sito ufficiale del Garante in merito al suo intervento alla conferenza "Neuroethics in a Time of Global Crises" in data 23 maggio 2022). Nell'ambito di un altro evento dedicato al tema (Giornata europea della privacy, "Privacy e neurodiritti. La persona al tempo delle neuroscienze" in data 28 gennaio 2021), il Prof. Stanzione aveva già messo in evidenza come proprio il cervello umano non possa essere ridotto a mero apparato biologico, alla luce delle profonde e forti connessioni tra esso e la coscienza e l'identità di ciascun individuo. In entrambi gli interventi viene messo in evidenza come le istanze di regolazione delle neurotecnologie nascono dal rilevare il possibile rischio che queste possano consentire, attraverso l'interpretazione sempre più precisa dei dati connessi alle funzioni cognitive, la lettura indiscriminata di stati mentali inespressi come intenzioni, emozioni e ricordi, incidendo negativamente propria sull'identità e dignità personale dei singoli fruitori. La possibilità che le neurotecnologie possano operare sulla capacità cognitiva, fino al punto di alterarla, diventa fattispecie tanto più rilevante da un punto di vista etico e giuridico laddove si consideri il progressivo diffondersi delle stesse anche in ambito extra-clinico. Il Presidente al riguardo ha fatto espresso riferimento a progetti di installazione di chip nel cervello con funzioni non solo di potenziamento cognitivo (funzioni ulteriori e transumane come il controllo telepatico di dispositivi) ma anche di selezione di ricordi (come nel caso della società Neuralink fondata da Elon Musk) o di condivisione di contenuti su social network direttamente con il pensiero (si pensi alle interfacce cervello-computer elaborato da Facebook nel 2018). La frontiera della profilazione dell'utente attraverso il neuromarketing, pertanto, risulterebbe in questi casi già ampiamente superata. Il Prof. Stanzione ha evidenziato come le neurotecnologie, infatti, non svolgano più soltanto una funzione essenzialmente analitico-descrittiva dei processi celebrali, ma potenzialmente siano in grado di manipolare il processo cognitivo fino al punto di predire possibili stati mentali (prevedendo il comportamento di ciascuno in base al suo comportamento passato), nonché di trattare dati per finalità di sfruttamento a fini commerciali delle informazioni così raccolte. Lo scenario innanzi prospettato rende evidente come tali tecnologie sono allo stato già in grado di incidere sul principio fondamentale di autodeterminazione individuale, con possibili conseguenze pregiudizievoli per la libertà cognitiva. Il Presidente precisa, infatti, che se in un futuro non troppo lontano le neurotecnologie potrebbero essere in grado di cogliere e decodificare anche i contenuti semantici dei nostri pensieri, ciò potrebbe comportare il venir meno della fondamentale ed essenziale segretezza del foro interno. Lo sviluppo della tecnologia applicata al cervello umano, laddove proseguisse senza alcuna regola o limite giuridico, non farebbe che aumentare e moltiplicare i rischi e le relative esigenze di tutela. Ciò soprattutto sul piano della capacità di discernimento, intesa come parametro valutativo fondamentale in ambito civilistico per l'applicazione delle misure a protezione dei soggetti privi in tutto o in parte di autonomia. Ad avviso del Presidente, a ciò si aggiunge un altro profilo centrale nel tema in questione, ovvero la volontarietà del fatto e la sua riconducibilità al soggetto agente (anche dal punto di vista della imputabilità penale). La questione in tale ultimo caso è quella della eterodeterminazione della condotta umana da parte dell'algoritmo: non solo il possibile hackeraggio del cervello ma anche la correttezza etica e giuridica di un intervento esterno sul processo cognitivo della persona umana. Nel senso di proporre un possibile metodo di analisi dei molteplici interrogativi e delle continue sfide poste dalle neurotecnologie da un punto di vista etico e giuridico, il Presidente distingue tra neurotecnologie mediche e neurotecnologie di consumo. Nel primo caso, viene sottolineata l'utilità di tali strumenti tecnologici al fine di prevenire, diagnosticare e/o contenere gli effetti invalidanti di determinate patologie; per tale motivo, occorre incoraggiarne la sempre più ampia diffusione, promuovendo il diritto a fruire delle possibilità offerte dal progresso tecnologico di cui all'art. 15 del Patto internazionale sui diritti economici, sociali e culturali. Ciò al fine di garantire una adeguata tutela del diritto fondamentale alla salute, fermo restando le indicazioni fornite sul punto dal Comitato Nazionale di Bioetica (documento del 2010 dal titolo "Neuroscienze ed esperimenti sull'uomo: osservazioni bioetiche"). Sul diverso versante delle neurotecnologie di consumo, invece, con espressione evocativa – capitalismo digitale – il Presidente Stanzione ha posto l'accento su una congiunzione tra neuroscienze e mercato che potrebbe avere implicazioni pregiudizievoli sulla vita dei singoli e della collettività. A dover essere messo sotto la lente di ingrandimento dell'interprete, in questa diversa fattispecie giuridicamente rilevante, è il rischio che esigenze di tutela di rango costituzionale (in primo luogo la dignità della persona), nonché la tutela di diritti fondamentali (come la privacy di chi si relaziona con devices neurotecnologici), siano disattese dal

concedere, senza alcuna regolamentazione, l'accesso indiscriminato alla parte più intima della persona: il suo substrato celebrale. Ciò in quanto, come precisa il Presidente, "nessun esercizio di diritto o libertà fondamentale potrebbe mai dirsi tale se realizzato per effetto del condizionamento, anche soltanto indiretto o parziale, da parte delle neurotecnologie sul processo cognitivo", né alcuna scelta individuale potrebbe mai definirsi veramente libera se presa per il timore della "trasparenza, della leggibilità, financo della predittività dei propri pensieri". Diventa, pertanto, necessario in tale contesto porre l'accento sulla possibilità che si individuino nell'ordinamento giuridico – creati ad hoc o anche solo desunti tramite interpretazione evolutiva – dei veri e propri neurodiritti quale possibile "statuto giuridico ed etico essenziale in base al quale coniugare l'innovazione e il diritto di fruire dei benefici offerti dal progresso scientifico con la dignità della persona". Nelle parole del Presidente, dunque, si coglie la necessità di fare riferimento a nuovi diritti di libertà come argine ad un uso improprio delle neurotecnolgie e che abbiano ad oggetto i processi cognitivi ed i dati ad essi connessi. Con specifico riferimento alla privacy, pertanto, la questione che si pone è quella di una diversa declinazione di tale diritto fondamentale, ampliando il raggio di tutela giuridica e focalizzando l'attenzione sul profilo informazionale del medesimo. Pertanto, prendendo le mosse dalla considerazione che "non tutto ciò che è tecnicamente possibile è anche giuridicamente lecito ed eticamente ammissibile", il Presidente conclude mettendo in evidenza il maggior rischio che occorre evitare: lo sviluppo di tecnologie che, nonostante abbiano un enorme potenziale positivo in termini di miglioramento della qualità della vita di persone con gravi disabilità, possono, per altro verso, diventare lo strumento per rendere l'uomo una "non-persona da addestrare, normalizzare o escludere".

ANNA ANITA MOLLO

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9770820

11. La proposta di uno 'US Stablecoin Trust Act' del U.S. Senate Banking Committee del 6 aprile 2022

Il 6 aprile 2022 Pat Toomey, membro del Congresso e dello U.S. Senate Banking Committee ha pubblicato una proposta di legge volta a delineare un quadro regolamentare a livello federale per la disciplina dei c.d. "*payment stablecoin*" (la "**Proposta**"). La Proposta ha ad oggetto una legge che prende il nome di "*The Stablecoin Trust Act*" e mira a stimolare lo sviluppo degli *stablecoins*, garantendo al contempo la protezione dei consumatori e la minimizzazione dei rischi per la stabilità finanziaria. La Proposta fa seguito ai principi generali per una disciplina degli *stablecoins* già delineati a dicembre 2021.

Al tempo, si era sottolineato come le iniziative di *stablecoins* si basassero su un modello di *business* diverso da quello dell'attività bancaria. Assoggettare gli *stablecoins* alla regolamentazione bancaria- come suggerito in alcune iniziative regolatorie al riguardo- ne avrebbe, quindi, soffocato lo sviluppo, a discapito dell'innovazione. Se ne erano, infatti, sottolineati i benefici, tanto da suggerire un ruolo degli *stablecoins* di supporto alla valuta ufficiale e di interoperabilità con il sistema finanziario.

La Proposta ha ad oggetto i soli *payment stablecoins*. In particolare, i *payment stablecoins* vengono definiti come valute virtuali convertibili- emesse centralmente e prive di interessi- il cui valore è stabilizzato in una o più valute di riferimento, permettendone un uso diffuso come mezzo di scambio.

Tre sono gli elementi chiave della Proposta. *In primis*, l'ambito di applicazione soggettivo, per cui possono emettere *stablecoins* solamente i *money transmitters*, i *national limited payment stablecoin issuers*; e, da ultimo, le *insured depository institutions*. La Proposta intende, quindi, preservare, da un lato, lo *status* degli emittenti già esistenti di *stablecoins*- in particolare, come *money transmitters*-e dall', altro, introdurre una categoria *ad hoc* con i nati*onal limited payment stablecoin issuers*. In particolare, quest'ultimi sarebbero regolati e autorizzati a livello federale, nonché soggetti alla supervisione dell'Office Comptroller Currency (OCC).

Secondo poi, la Proposta definisce dei *regulatory standards* generali da applicarsi a tutti i soggetti a cui è permessa l'attività di emissione degli *stablecoins*, così da garantire la protezione dei consumatori. Tali *regulatory standards* consistono perlopiù n requisiti informativi aventi ad oggetto le attività detenute a riserva dall'emittente e la relativa composizione, nonché le politiche di rimborso. Si prevede anche la predisposizione di una relazione su base trimestrale da parte di una società di revisione contabile a conferma che le attività di riserva non divergano da quanto dichiarato dall'emittente. In aggiunta, la Proposta prevede dei *regulatory standards* specifici per i *national limited stablecoin issuers* dati da requisiti di capitale,

requisiti di liquidità e requisiti riguardanti la gestione del rischio e la struttura di *governance*, la cui definizione sarebbe rimessa all'OCC. Requisiti specifici si hanno anche rispetto le attività di riserva e la relativa composizione. In particolare, i *national limited stablecoin issuers* dovranno detenere attività di riserva aventi un valore di mercato almeno pari al valore nominale aggregato degli *stablecoins* emessi e circolanti. Le attività di riserva dovrebbero limitarsi a contante o strumenti equivalenti o ad attività altamente liquidabili. La Proposta prevede l'accesso dei *national limited payment stablecoin issuers* ai *master accounts* e ai servizi della Federal Reserve, predisponendo, quindi, una prima rete di protezione.

Da ultimo, la Proposta si propone di escludere e chiarire espressamente come i *payment stablecoins* non siano da considerarsi *securities* fintantoché siano privi di interessi e come, quindi, non sarebbero soggetti al raggio d'azione della *Securities Exchange Commission* (SEC).

ALICE FILIPPETTA

https://www.banking.senate.gov/newsroom/minority/toomey-announces-legislation-to-create-responsible-regulatory-framework-for-stablecoins

https://www.banking.senate.gov/imo/media/doc/the_stablecoin_trust_act.pdf

12. La sentenza del Tribunale di Milano del 20 aprile 2022 su algoritmo e qualificazione del rapporto di lavoro subordinato: il caso Deliveroo (Trib. Milano sentenza n. 1018/2022)

Con la sentenza n. 1018 del 20.04.2022, il Tribunale di Milano (sez. lavoro), nella persona del giudice dott. Franco Caroleo (di seguito, solo, rispettivamente, la "**Sentenza**" e il "**Tribunale**"), si è pronunciato sul tema della natura giuridica del rapporto di lavoro riguardante i lavoratori della c.d. *gig economy*, in una particolare fattispecie riguardante la nota piattaforma Deliveroo (di seguito la "**Piattaforma**") gestita dall'omonima società (la "**Società**"), stabilendo che i medesimi lavoratori (c.d. *rider*) non possano essere inquadrati come lavoratori autonomi qualora la prestazione da eseguire sia gestita in maniera dettagliata e cogente dall'algoritmo in particolare relativamente alla distribuzione dei turni di disponibilità dei *rider* compiuta settimanalmente attraverso apposita prenotazione *online* da effettuarsi da parte degli stessi *rider* in un solo giorno della settimana stabilito dalla Società ed in determinate fasce orarie sempre predeterminate dalla Società e dalla stessa rese accessibili o inaccessibili ai vari *rider* sulla base di criteri premiali, sempre predeterminati dal datore di lavoro. La vicenda in oggetto originava allorché un *rider*, dopo aver stipulato, in data 01.12.2018, un *"contratto di lavoro autonomo"* con la Società, la evocava in giudizio affinché venisse riconosciuta, in via principale, la natura subordinata di detto rapporto di lavoro o, quantomeno, in via subordinata, l'applicazione delle garanzie previste dall' art. 2, comma 1, del D.Lgs. 81/2015, a norma del quale la disciplina del rapporto di lavoro subordinato si applica anche ai rapporti di collaborazione che hanno ad oggetto prestazioni di lavoro *"a carattere esclusivamente personale e continuativo, mediante modalità di esecuzione organizzate dal committente con riferimento a tempi e luoghi di lavoro"* (Cass. 1663/2020). La società convenuta, costituitasi in giudizio, contestava le pretese avversarie e chiedeva la reiezione del ricorso facendo leva sulla libertà concessa al *rider*, nella sessione di turni di disponibilità da lui prenotata, di accettare, ignorare o rifiutare le singole proposte. Le argomentazioni di parte attrice, peraltro in linea con le risultanze probatorie, le testimonianze rese e la documentazione in atti, hanno però indotto il Tribunale a ritenere che questa attività lavorativa abbia i connotati propri della subordinazione. Nella Sentenza vengono in primo luogo ricordati e citati numerosi passaggi dell'importante sentenza già sopra ricordata (Cass. 1663/2020) ed il suo valore nomofilattico nella materia sottoposta al giudizio del Tribunale. In particolare, nella Sentenza si ricorda che nella predetta pronuncia la Corte di Cassazione, oltre che essersi soffermata sulle condizioni necessarie e sufficienti per applicare le garanzie di cui all' art. 2, comma 1, del D.Lgs. 81/2015, abbia anche riconosciuto espressamente che al giudice di merito non è in alcun modo precluso l'accertamento dei requisiti di una subordinazione a fronte di una specifica domanda della parte interessata fondata sui parametri normativi dell'art. 2094 c.c. Nello specifico, valorizzando le allegazioni e il materiale probatorio in atti, il Tribunale ha argomentato che se da un lato è vero che il *rider*, dopo aver scaricato l'app e aver ricevuto sul proprio *smartphone* delle credenziali (*login* e *password*) per accedere alla Piattaforma, possa rendersi disponibile a ricevere proposte di consegna nelle sessioni di lavoro da lui prenotate (tra quelle disponibili al momento della prenotazione), e possa poi rifiutare le singole proposte di consegna ricevute durante quelle sessioni, è pur vero che la suddetta prenotazione dei turni di disponibilità del *rider* debba essere dal

medesimo *rider* inderogabilmente effettuata sulla Piattaforma ogni lunedì collegandosi *online* in una precisa fascia oraria tra le tre fasce orarie (alle ore 11.:00, o 13:00 o 15:00) previste dalla Società, e che l'accesso ad una piuttosto che ad un'altra fascia oraria viene stabilito dalla Società in base a criteri o indici da essa predeterminati e gestiti da un algoritmo. Questi, denominati indici *self-service booking* o indici SSB, vengono determinati da due fattori. Il primo è quello relativo all'affidabilità o inaffidabilità del *rider*, intese come indici statistici volti ad individuare il numero di volte in cui il *rider*, dopo aver prenotato una sessione, ha effettuato o non ha effettuato il *login* entro i primi 15 minuti della medesima sessione. Il secondo riguarda invece la partecipazione del *rider* alle sessioni in cui ci sono più richieste di consegne da parte dei clienti e consiste nel premiare (attribuendo un punteggio o *ranking* maggiore rispetto agli altri lavoratori), solo i *rider* che hanno scelto di lavorare tra venerdì e domenica nella fascia oraria compresa tra le ore 20:00 e le ore 22:00. L'accesso alla prima fascia di prenotazione (ore 11:00) è migliore rispetto all'accesso alle due successive fasce di prenotazione, perché consente ai *rider* una maggiore scelta tra i turni di lavoro (sessioni) disponibili nel corso della settimana. A sua volta, e per lo stesso motivo, la fascia delle 13:00 è migliore di quella delle 15:00. Secondo quanto il Tribunale ha desunto dal materiale probatorio, l'accesso alla fascia delle 11:00 risultava consentito solo ai *rider* che presentavano un valore massimo degli indici suddetti. Il Tribunale ha argomentato che tale previsione non si configura soltanto come espressione di un potere disciplinare bensì rappresenta una sintomatica manifestazione di un più generale potere direttivo della società. Secondo il Tribunale, a ciò si aggiungono altri elementi sulla base dei quali è stato conclusivamente argomentato che la prestazione in esame risultasse *"completamente organizzata dall'esterno, con un'incidenza diretta sulla modalità di esecuzione, sui tempi e sui luoghi"*. Tra questi, in particolare, l'attività di monitoraggio della Società sul *rider*, che avviene mediante un sistema di geolocalizzazione, e la condizione per cui, poter ricevere la proposta, il *rider* deve obbligatoriamente trovarsi all'interno della zona in cui ha prenotato la sessione. È dunque emerso come la prestazione del lavoratore, organizzata e gestita essenzialmente dall'algoritmo (in particolare per quanto attiene alle modalità di assegnazione degli incarichi di consegna), risultasse svolta *"per le finalità di un'organizzazione della società titolare della piattaforma sulla quale il rider non può esercitare alcuna influenza*". In considerazione di quanto sopra, il Tribunale non ha ritenuto sufficiente al fine di escludere la subordinazione, la circostanza che il *rider* potesse ignorare o non accettare le singole proposte di consegna inviategli dalla Società nelle sessioni da egli prenotate. Tale circostanza, secondo il Tribunale, pur essendo espressione del consenso del lavoratore, deve, nel contesto fattuale specifico, ritenersi come rappresentativa di un elemento esterno al contenuto del rapporto e idoneo, dunque, ad incidere non sulla forma e sul contenuto della prestazione ma sulla sua costituzione e durata. In più, il Tribunale ha revocato in dubbio che il *rider*, nell'organizzazione del lavoro sopra descritta, potesse ritenersi veramente 'libero' nelle sue determinazioni, atteso che l'accesso alle fasce orarie disponibili per prenotare le sessioni di lavoro settimanali dipendevano da fattori predeterminati ed imposti dalla Società, uno dei quali in particolare (il rendersi disponibile a lavorare nel fine settimana tra le 20:00 e le 22:00) era in questo senso chiaramente condizionante; e che soltanto la prima fascia oraria del lunedì (quella delle ore 11:00) consentiva davvero al *rider* di scegliere tra tutti i turni disponibili, ma era a sua volta accessibile in base ad un meccanismo di punteggio che prevedeva prestazioni predeterminate dalla Società.

Sulla base degli elementi appena descritti il Tribunale ha accertato e dichiarato che tra le parti è intercorso - nel tempo in cui l'organizzazione del lavoro aveva i caratteri sopra sommariamente descritti (i.e. necessità che il *rider* effettuasse un *login* per prenotare i turni di disponibilità lavorativa solo il lunedì in una delle tre fasce orarie prefissate dalla Società ed accessibili o inaccessibili al *rider* sulla base dei sopra descritti indici o criteri di c.d. *self-service booking* predeterminati ed imposti dalla medesima Società e gestiti da un algoritmo, con le conseguenti statistiche e *ranking*) - l'esistenza di un rapporto di lavoro subordinato a tempo pieno ed indeterminato con riferimento al quale trova operatività il CCNL Commercio di livello 6, ove sono collocati i lavoratori le cui prestazioni richiedono il possesso di *"semplici conoscenze pratiche"*.

Degno di nota è che nella Sentenza il Tribunale ha fatto anche riferimento a giurisprudenza straniera recente su casi simili, in particolare a giurisprudenza spagnola e olandese (cfr. in particolare punti 7.1, 7.4, 7.5 e 7.7 della Sentenza).

Si osserva infine che nella Sentenza si dà conto – nella parte relativa alle prove testimoniali - che la Società avrebbe dal 2020 in poi mutato l'organizzazione del lavoro relativamente alla prenotazione dei turni di disponibilità, consentendo a tal fine ai *rider* un accesso (*login*) al sistema per prenotare le sessioni di lavoro in qualunque

momento (c.d. *free-login*) in luogo del sistema gestito dagli indici di *self-service booking* sopra descritti.

VINCENZO PITTELLI

https://web.uniroma1.it/deap/sites/default/files/allegati/Trib.Milano_Sentenza_1018_20.04.2022.pdf