



# **Atlante storico del diritto dei dati** **Anni 2020-2022**

Raccolta della rubrica *Diritto e nuove tecnologie*  
pubblicata sulla rivista *Persona e Mercato*  
dall'Osservatorio Giuridico sull'Innovazione Digitale

a cura di Salvatore Orlando e Mario Mauro



PERSONA E MERCATO

***Atlante storico del diritto dei dati. Anni 2020-2022*, a cura di Salvatore Orlando e Mario Mauro, Persona e Mercato ed., Firenze, 2023**

ISBN 978-88-947441-2-5

Il presente volume è concesso in licenza Creative Commons [CC-BY-SA-4.0](https://creativecommons.org/licenses/by-sa/4.0/)

L'immagine in copertina dal titolo "Studio 2023 sul logo OGID-JODI" è di Michela Tenace, archivio dell'autore - diritti riservati.

# PRESENTAZIONE

Siamo lieti di presentare in un'unica opera facilmente consultabile anche attraverso appositi indici in fondo al volume ([per anno](#), [per Autore](#) e [analitico](#)) dotati di collegamenti ai testi, i contributi dei primi tre anni della rubrica *Diritto e nuove tecnologie* pubblicata sulla rivista [Persona e mercato](#).

Scorrendo gli indici e i titoli dei contributi, si conferma l'opportunità che a suo tempo ha motivato l'idea di promuovere e coordinare il lavoro della rubrica in seno alle attività dell'[Osservatorio Giuridico sull'Innovazione Digitale](#).

Ed effettivamente, il quadro d'insieme, che oggi presentiamo ai lettori, restituisce l'immagine di un vero e proprio atlante storico delle principali notizie che si sono succedute nel corso degli ultimi tre anni nell'ormai vasto settore del diritto che può chiamarsi *Diritto dei dati*, avente ad oggetto il governo dei nuovi e specifici conflitti di interessi creati dal peculiare impatto esercitato sui rapporti tra i privati e tra questi e le autorità pubbliche dalle incessanti innovazioni delle tecnologie digitali.

Si tratta di 128 contributi scritti da 40 autori. Ad essi va il nostro ringraziamento, nella speranza di poter proseguire nell'opera.

Luglio 2023

I curatori



## COLLEGAMENTI

[Anno 2020](#)

[Anno 2021](#)

[Anno 2022](#)

[Indici per anni](#)

[Indice per Autore](#)

[Indice analitico](#)



## ANNO 2020

<a href="#">2020/1(1)RM</a>	
L'utilizzo dei droni ai tempi del coronavirus – La Nota ENAC del 23 marzo 2020 e il successivo stop del Dipartimento della Pubblica Sicurezza del Ministero dell'Interno .....	p. 5
<a href="#">2020/1(2)MP</a>	
Diritto societario e Coronavirus: intervento e verbalizzazione assembleare a distanza .....	p. 6
<a href="#">2020/1(3)EMI</a>	
Regno Unito: quale futuro per crypto-asset e smart contract? .....	p. 7
<a href="#">2020/1(4)MG</a>	
Dati personali e valore economico – il Tar Lazio conferma l'importante provvedimento dell'Antitrust nel caso Facebook .....	p. 8
<a href="#">2020/1(5)SO</a>	
Il Libro Bianco della Commissione Europea del 19 febbraio 2020 sull'Intelligenza Artificiale: “Eccellenza e Fiducia” .....	p. 9
<a href="#">2020/1(6)DI</a>	
Intelligenza Artificiale e Costituzione francese .....	p. 10
<a href="#">2020/1(7)LC</a>	
Rome Call for AI Ethics: Per un'intelligenza artificiale umanistica .....	p. 11
<a href="#">2020/1(8)EWDM</a>	
Le Linee Guide AGID del 23 marzo 2020 - Il valore giuridico della firma con il Sistema Pubblico d'identità Digitale (SPiD) .....	p. 12
<a href="#">2020/2(1)FR</a>	
La Comunicazione della Commissione europea COM(2020) 66 final “Una strategia europea per i dati” .....	p. 13
<a href="#">2020/2(2)CR</a>	
I lavori del 12 maggio 2020 della Commissione giuridica (JURI) del Parlamento Europeo sulla regolazione della Intelligenza Artificiale: il Draft Report sugli aspetti etici .....	p. 15
<a href="#">2020/2(3)SO</a>	
(segue): il Draft Report sulla responsabilità civile .....	p. 16
<a href="#">2020/2(4)LC</a>	
(segue): il Draft Report sulla proprietà intellettuale .....	p. 18
<a href="#">2020/2(5)EMI</a>	
Le linee guida del EDPB sul consenso: chiarimenti su <i>cookie wall</i> e scorrimento dei siti web .....	p. 20
<a href="#">2020/2(6)DI</a>	
Una nuova legge francese sui contenuti offensivi sul web .....	p. 21
<a href="#">2020/2(7)MP</a>	
Il (primo) parere del Garante per la protezione dei dati personali sull'applicazione volta al tracciamento dei contagi da Covid-19 .....	p. 22

<a href="#">2020/2(8)EP</a>	Stablecoin globali: prospettive regolamentari e rischi finanziari sotto la lente della BCE .....	p. 23
<a href="#">2020/3(1)CR</a>	La sentenza “Schrems II” del 16 luglio 2020 della Corte di Giustizia UE sul Privacy Shield con gli USA e sulle clausole contrattuali tipo .....	p. 25
<a href="#">2020/3(2)FB</a>	Le conclusioni dell'Avvocato generale della Corte di Giustizia UE del 16 luglio 2020 sull'interpretazione delle direttive 2001/29/CE e 2000/31/CE sulla responsabilità dei gestori di piattaforme online con riferimento alle opere protette dal diritto d'autore .....	p. 26
<a href="#">2020/3(3)LC</a>	CasaPound vs. Facebook: il Tribunale di Roma conferma in sede di reclamo il provvedimento cautelare a favore di CasaPound .....	p. 30
<a href="#">2020/3(4)FP</a>	Pubblicate il 10 luglio 2020 la relazione introduttiva e le prime tre bozze di relazione del gruppo di esperti dell' <i>Observatory on the Online Platform Economy</i> .....	p. 31
<a href="#">2020/3(5)EWDM</a>	Lo studio del luglio 2020 su “Intelligenza Artificiale e responsabilità civile” commissionato dalla Commissione JURI del Parlamento europeo .....	p. 34
<a href="#">2020/3(6)SG</a>	Il Consiglio di Stato francese conferma la sanzione di 50 milioni di Euro a Google per violazione del GDPR .....	p. 36
<a href="#">2020/3(7)EMI</a>	La « <i>Algorithm Charter</i> » della Nuova Zelanda .....	p. 37
<a href="#">2020/4(1)SG</a>	La risoluzione del Parlamento europeo del 20 ottobre 2020 sul regime di responsabilità civile per l'intelligenza artificiale .....	p. 39
<a href="#">2020/4(2)MS</a>	La proposta della Commissione europea del 24 settembre 2020 avente ad oggetto l'emanazione di un Regolamento Europeo sui Mercati di Criptoattività (MiCAR) .....	p. 41
<a href="#">2020/4(3)MP</a>	La prima sentenza della Corte di Giustizia UE sul principio di «neutralità di Internet» ai sensi del regolamento (UE) 2015/2120 .....	p. 44
<a href="#">2020/4(4)CM</a>	La lunga marcia verso il GDPR cinese: la prima legge sulla protezione delle informazioni personali della Repubblica popolare nella bozza per i commenti pubblici del 21 ottobre 2020 .....	p. 46
<a href="#">2020/4(5)CR</a>	Le FAQ del Garante Privacy italiano dell'ottobre 2020 per la protezione dei dati personali sulla refertazione online .....	p. 47
<a href="#">2020/4(6)DPDM</a>	La nuova indagine della Commissione europea per abuso di posizione dominante di Amazon .....	p. 48
<a href="#">2020/4(7)LC</a>	Droits voisins e snippets: la Corte d'appello di Parigi conferma la decisione dell'Autorità garante della concorrenza francese nei confronti di Google .....	p. 49

[2020/4\(8\)SO](#)

La Sapienza sottoscrive “Rome Call for AI Ethics” ..... p. 50



2020/1(1)RM

### **L'utilizzo dei droni ai tempi del coronavirus – La Nota ENAC del 23 marzo 2020 e il successivo stop del Dipartimento della Pubblica Sicurezza del Ministero dell'Interno**

Il ricorso alla tecnologia dei droni, considerata idonea a consentire un maggior rispetto delle misure coattive volte al contenimento e al contrasto dell'emergenza epidemiologica da "coronavirus", è al centro di una nota dell'ENAC (Ente Nazionale per l'Aviazione Civile) del 23 marzo 2020 (la "Nota"). Procedendo dal richiamo della generale finalità di garantire il contenimento dell'emergenza epidemiologica "coronavirus," ed enunciando, più specificamente, il fine di consentire le operazioni di monitoraggio degli spostamenti dei cittadini sul territorio comunale, prevista dai D.P.C.M. 8 e 9 marzo 2020, l'ENAC, attraverso la Nota - dopo aver dichiarato espressamente di aver operato sulla scorta delle «esigenze manifestate da numerosi Comandi di Polizie Locali» - ha ritenuto necessario procedere a derogare ad alcune previsioni delle disposizioni del Regolamento ENAC "Mezzi Aerei a Pilotaggio Remoto" Edizione 3 del 11 novembre 2019 (il "Regolamento").

In particolare, la Nota ha disposto che, fino al 3 aprile 2020, «le operazioni condotte con sistemi aeromobili a pilotaggio remoto con mezzi aerei di massa operativa al decollo inferiore a 25 kg, nella disponibilità dei Comandi di Polizia Locale ed impiegati per le sopra indicate attività di monitoraggio, potranno essere condotte in deroga ai requisiti di registrazione e di identificazione di cui all'art. 8 del citato Regolamento».

Inoltre, in deroga all'art. 10 del Regolamento e con riferimento alle operazioni critiche, la Nota ha stabilito che queste potranno essere effettuate in *Visual Line of Sight* - ossia mantenendo costantemente il contatto visivo con il drone stesso - «anche su aree urbane dove vi è scarsa popolazione esposta al rischio di impatto; non sarà altresì necessario il rilascio di autorizzazione da parte di questo Ente e non sarà richiesta la rispondenza delle operazioni agli scenari standard pubblicati».

Infine, la Nota precisa che i droni degli Enti di Stato di cui all'art. 744 del Codice della Navigazione e delle Polizie Locali dei Comuni italiani, «se impiegati nell'ambito delle condizioni emergenziali dovute all'epidemia COVID-19», potranno volare anche in aree prospicienti agli aeroporti civili, identificate come "aree rosse", fino ad una quota massima di 15 metri. In questi casi sarà necessaria una comunicazione preventiva alla torre di controllo dell'aeroporto e si dovrà comunque dare «sempre priorità al traffico degli aeromobili da/verso gli aeroporti».

La capacità dei droni di volare a lunga distanza e l'installazione su essi di telecamere ad alta risoluzione consentono di verificare, in tempo reale, eventuali assembramenti di persone e spostamenti non autorizzati, così da consentire tempestivamente interventi e operazioni di sicurezza da parte delle Forze dell'Ordine. Sulla base di tale constatazione, le Polizie Locali hanno manifestato all'ENAC le esigenze di intervento, che, come detto, sono state considerate dall'ENAC per l'adozione della Nota.

Tuttavia, secondo fonti giornalistiche accreditate, qualche giorno dopo l'adozione della Nota, il capo del Dipartimento della Pubblica Sicurezza presso il Ministero dell'Interno ha ordinato uno stop alle disposizioni di cui alla Nota, in attesa di approfondimenti in corso con l'ENAC e che sarebbero finalizzati alla verifica della corretta applicazione delle procedure di impiego dei droni, in particolare ad opera delle forze di Polizia municipale.

ROSARIA MANAGÒ

<https://www.enac.gov.it/news/aggiornamento-del-24-marzo-2020-utilizzo-droni-provvedimenti-governativi-emergenziali-in>

2020/1(2)MP

### **Diritto societario e Coronavirus: intervento e verbalizzazione assembleare a distanza.**

Il Consiglio Notarile di Milano con la massima 187 dell'11 marzo 2020, emanata in relazione al contenuto dall'articolo 1, comma 1, lettera q) del D.P.C.M. dell'8 marzo 2020 - il quale dispone che «sono adottate, in tutti i casi possibili, nello svolgimento di riunioni, modalità di collegamento da remoto» - ha dettato un principio di comportamento per lo svolgimento delle riunioni assembleari, in seduta ordinaria e straordinaria, a distanza.

L'intervento in assemblea mediante mezzi di telecomunicazione, ove consentito dallo statuto ai sensi dell'art. 2370, comma 4, c.c., o comunque ammesso dalla vigente disciplina - può ora pacificamente riguardare la totalità dei partecipanti alla riunione, ivi compreso il presidente.

Ai sensi dell'art 2370, comma 4, c.c. è infatti possibile l'intervento all'assemblea mediante mezzi audio o video, subordinatamente alla sussistenza di una clausola dello statuto che consenta l'intervento con le modalità suddette (clausola in realtà non indispensabile per le società chiuse secondo il Comitato Triveneto dei Notai, massima H.B. 39), ferma restando la necessità di garantire l'identificazione e la corretta partecipazione al dibattito assembleare e alla votazione degli intervenuti a distanza. Si riteneva, nel silenzio del legislatore, che la legittimità della conference call fosse comunque subordinata alla presenza nel luogo di convocazione dell'assemblea del presidente della riunione e del segretario o del notaio verbalizzante.

Con la Massima 187 è stata invece riconosciuta legittimità allo svolgimento della riunione societaria in full audio conference, con tutti i partecipanti al telefono o connessi in video conferenza, ivi compreso il Presidente.

Resta fermo che nel luogo indicato nell'avviso di convocazione deve trovarsi il segretario verbalizzante o il notaio, qualora si tratti di assemblea straordinaria, unitamente alla o alle persone incaricate dal presidente per l'accertamento dell'identità e della legittimazione di coloro che intervengono di persona. Quest'ultimo incarico può tuttavia essere affidato al segretario verbalizzante o al notaio, così che è ammessa la possibilità che tutti i partecipanti all'adunanza si trovino in luoghi diversi.

Secondo i notai milanesi, le clausole statutarie che prevedono la presenza del presidente e del segretario nel luogo di convocazione (o comunque nel medesimo luogo) devono intendersi funzionali alla formazione contestuale del verbale dell'assemblea, sottoscritto sia dal presidente sia dal segretario. Esse pertanto non impediscono lo svolgimento della riunione assembleare con l'intervento di tutti i partecipanti mediante mezzi di telecomunicazione, potendosi in tal caso redigere successivamente il verbale assembleare, con la sottoscrizione del presidente e del segretario, oppure con la sottoscrizione del solo notaio in caso di verbale in forma pubblica. La Massima 187 si colloca così nel solco dell'orientamento che afferma la validità del verbale postumo sottoscritto dal solo pubblico ufficiale.

Altresì, ancorché in assenza della clausola statutaria suddetta, a seguito del D.P.C.M. dell'8 marzo 2020 è da ritenere consentita la riunione assembleare in conference call anche laddove

non espressamente contemplata e legittimata da clausola statutaria. Non solo: il principio trova applicazione anche per le riunioni dell'organo amministrativo, stante il disposto del comma 1 dell'art 2388 c.c.

MICHELA PAGANELLI

<https://www.consiglionotarilemilano.it/notai/massime-commissione-societa.aspx>

2020/1(3)EMI

### **Regno Unito: quale futuro per *crypto-asset* e *smart contract*?**

Il 18 novembre 2019 la *Jurisdictional Taskforce* del Regno Unito (UKJT) ha pubblicato un “*Legal Statement*” con l’obiettivo di inquadrare i complessi fenomeni dei *crypto-asset* e degli *smart contract* all’interno dell’ordinamento giuridico anglosassone. Il documento, diviso in due sezioni, si interroga, da un lato, sulla veste giuridica degli asset crittografici e, dall’altro, sulla potenziale vincolatività legale degli *smart contract*.

In merito alla prima questione, gli autori del documento non si spingono a definire cosa si intenda per *crypto-asset*, ma si limitano a identificarli come fenomeni informatici capaci di sintetizzare crittograficamente asset di vario genere. Il documento afferma che essi vadano interpretati al pari di altri asset proprietari intangibili dotati di un certo grado di *permanence* e *stability*, seguendo i profili definatori ed i criteri interpretativi individuati nella controversia *National Provincial Bank v. Ainsworth H/L [1965] A.C. 1175* e confermati successivamente da consolidata giurisprudenza, e, in particolare, dal caso *Fairstar Heavy Transport NV v. Adkins [2013] EWCA Civ 886*. Lo studio mira a puntualizzare che questi asset non possano essere classificati né come *things in action* né come *things in possession*, in linea con la storica distinzione elaborata nel caso *Colonial Bank v. Whinney [1885]*. Infatti, come si sottolinea nello Statement, questi asset virtuali non possono essere oggetto di possesso fisico né, tantomeno, essere considerati come mere informazioni, documenti o titoli, ma possono essere, invece, oggetto di specifici diritti. A tal riguardo, si mette in luce che tali diritti presentano le caratteristiche di certezza, esclusività, trasferibilità e controllo, tipiche dei tradizionali *property rights*. Più specificatamente, le suddette caratteristiche sono garantite da un sistema di identificabilità del titolare dell’asset intangibile tramite il ricorso a chiavi crittografiche riferibili ad un unico soggetto.

Con riferimento agli *smart contract*, invece, il documento pone attenzione alle loro principali peculiarità tecniche, tra cui, su tutte, quella della “automaticità” (*automaticity*) della loro esecuzione. Tale carattere viene desunto sulla base della constatazione che gli *smart contract* vengono eseguiti senza alcun tipo di intervento umano. Sul punto, gli autori sostengono che possa rientrare in tale categoria sia il contratto meramente eseguito attraverso sistemi algoritmici sia il contratto le cui prestazioni ed obbligazioni siano interamente rappresentate dal codice informatico. Inoltre, si legge che gli *smart contract* sembrano presentare i requisiti minimi per la conclusione di un contratto secondo le regole di *common law*, tra cui, di particolare rilievo ai fini dello studio in esame, il raggiungimento di un accordo contrattuale chiaro a cui le parti si vincolano. Secondo gli autori dello *statement*, gli *smart contract* devono, dunque, essere interpretati secondo i tradizionali principi del diritto inglese, adattandoli alle specificità tecnologiche di questi strumenti ma ricercando, sempre, l’effettiva volontà delle parti, anche altrove esplicitata.

Questo studio, sebbene non possa essere considerato come *binding law* nell'ordinamento del Regno Unito, offre, allo stesso tempo, spunti di approfondimento e chiavi di lettura tali da poter condizionare la futura evoluzione del diritto anglosassone, nonché una evidente apertura del sistema inglese al recepimento giuridico di questi fenomeni tecnologici.

ENZO MARIA INCUTTI

<https://technation.io/about-us/lawtech-panel>

2020/1(4)MG

### **Dati personali e valore economico – il Tar Lazio conferma l'importante provvedimento dell'Antitrust nel caso Facebook**

Con la sentenza n. 261 del 18 dicembre 2019 – 10 gennaio 2020, Il Tar Lazio, Sez. I ha confermato la legittimità del provvedimento con il quale in data 6 aprile 2018 l'Autorità Garante della Concorrenza e del Mercato (“Agcm”) ha sanzionato Facebook Inc. e *Facebook Ireland Limited* rilevando che l'utente, che accede alla homepage di *Facebook* per registrarsi, trova un *claim* sulla gratuità del servizio offerto “Iscriviti è gratis e lo sarà per sempre”, ma non anche un altrettanto evidente e chiaro avvertimento sul successivo utilizzo dei dati a fini commerciali da parte di Facebook. Codesta condotta è ritenuta una pratica commerciale ingannevole ai sensi degli artt. 21 e 22 del decreto legislativo n. 206 del 6 settembre 2005 (cd. “Codice del Consumo”).

Avverso il provvedimento *Facebook Inc* ha presentato ricorso, tra l'altro, contestando:

1. il difetto di competenza dell'Agcom, in quanto non sussiste alcuna pratica commerciale in mancanza di un corrispettivo patrimoniale richiesto all'utente (Direttiva 2005/29/CE);
2. il difetto di attribuzione dell'Agcom, “*ratione materiae*”, in quanto la questione attiene all'uso di dati personali ed è perciò assorbita dalla disciplina della privacy (Regolamento UE 2016/679) sulla base del principio di specialità di cui all'art. 3, comma 4, della Direttiva sulle pratiche commerciali sleali;
3. la violazione del principio di legalità e prevedibilità, in quanto Facebook è stata sanzionata sulla base di una disciplina – le pratiche commerciali scorrette – la cui applicazione al tema della gestione dei dati personali è imprevedibile e nuova, e quindi in forza di una interpretazione estensiva della disciplina vietata dall'art. 7 CEDU;
4. l'inesistenza di qualsiasi pratica commerciale scorretta, in quanto i consumatori medi non sono fuorviati dalla indicazione del servizio come “gratuito”.

La sentenza del Tar Lazio n. 261/20 ha respinto le doglianze del ricorrente per le seguenti ragioni:

1. non è condivisibile la carenza di potere dell'Agcom, sostenendo che avrebbe invaso un campo di competenza dell'Autorità Garante per la Privacy. Infatti, a fronte della protezione del dato personale quale espressione di un diritto della personalità dell'individuo, tutelato dalla disciplina della privacy, sussiste anche un diverso campo di protezione del dato, quando questo diviene oggetto di una compravendita tra gli operatori del mercato. Quest'ultima ipotesi si realizzerebbe proprio nel caso di specie, atteso che la raccolta e lo sfruttamento dei dati degli utenti a fini remunerativi da parte di *Facebook* configurerebbe la contro-prestazione del servizio offerto dal social network;

2. deve anche escludersi che l'omessa informazione sullo sfruttamento ai fini commerciali dei dati dell'utente sia una questione interamente disciplinata e sanzionata nella disciplina della privacy (come già dimostrato, tra l'altro, dalla Corte di giustizia dell'Unione Europea, del 13 settembre 2018, nelle cause riunite C 54/17 e C 55/17, nella quale si era statuito che la disciplina consumeristica non trova applicazione "unicamente quando disposizioni estranee a quest'ultima, disciplinanti aspetti specifici delle pratiche commerciali sleali, impongono ai professionisti, senza alcun margine di manovra, obblighi incompatibili con quelli stabiliti dalla Direttiva 2005/29/CE);
3. la possibilità di sfruttare economicamente il dato personale nell'ambito delle piattaforme social e la conseguente necessità di tutelare il consumatore non può neppure definirsi innovativo e frutto di una interpretazione "estensiva" di norme sanzionatorie, come tale contraria al principio di prevedibilità (ad esempio, già negli "Orientamenti per l'attuazione/applicazione della Direttiva 2005/29/CE relativa alle pratiche commerciali sleali" del 25 maggio 2016, la Commissione Europea aveva affermato che "i dati personali, le preferenze dei consumatori e altri contenuti generati dagli utenti hanno un valore economico de facto");
4. la condotta sanzionata si presenta come ingannevole, in quanto il "claim" utilizzato da Facebook nella pagina di registrazione per invogliare gli utenti ad iscriversi ("Iscriviti E' gratis e lo sarà per sempre") lascia intendere l'assenza di una controprestazione richiesta al consumatore in cambio della fruizione del servizio.

In ultimo, la pronuncia del TAR statuisce che «Il fenomeno della "patrimonializzazione" del dato personale, tipico delle nuove economie dei mercati digitali, impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere reso edotto dello scambio di prestazioni che è sotteso alla adesione ad un contratto per la fruizione di un servizio, quale è quello di utilizzo di un "social network».

MARISTELLA GIANNINI

<https://www.giustizia-amministrativa.it/provvedimenti-tar-roma>.

2020/1(5)SO

### **Il Libro Bianco della Commissione Europea del 19 febbraio 2020 sull'Intelligenza Artificiale: "Eccellenza e Fiducia"**

Il 19 febbraio 2020 la Commissione Europea ha pubblicato un *White Paper* sull'intelligenza artificiale contenente una serie di proposte per lo sviluppo programmatico di due piani di azione, individuati, rispettivamente, con le parole "eccellenza" e "fiducia".

Dopo aver dichiarato in premessa che le tecnologie dell'intelligenza artificiale ("IA") si stanno sviluppando rapidamente e che esse apporteranno notevoli vantaggi alla vita di tutti i cittadini, a partire dall'ambito dell'assistenza sanitaria e della prevenzione delle malattie, il Libro Bianco propone: (a) attraverso l'obiettivo programmatico dell'eccellenza, una serie di azioni intese a rendere competitive le imprese europee - ed in particolare le piccole e medie imprese ("PMI") europee - attive nel settore dell'IA; e (b) attraverso l'obiettivo

programmatico della fiducia, una serie di azioni intese a fissare le politiche di regolazione delle tecnologie dell'IA.

Sotto quest'ultimo aspetto, il Libro Bianco, dopo aver collegato l'esigenza di una regolazione alla necessità di creare maggiore fiducia dei cittadini nelle applicazioni dell'IA, ha richiamato i risultati raggiunti dal “gruppo di esperti di alto livello”, la cui condivisione da parte della Commissione Europea è contenuta nella comunicazione “COM(2019) 168 final”, sotto forma dei c.d sette requisiti fondamentali:

- intervento e sorveglianza umani,
- robustezza tecnica e sicurezza,
- riservatezza e governance dei dati,
- trasparenza,
- diversità, non discriminazione ed equità (o correttezza: “*fairness*” nel testo inglese),
- benessere sociale e ambientale, e
- accountability.

La struttura degli interventi proposti nel Libro Bianco procede dalla distinzione tra applicazioni di IA “ad alto rischio” e applicazioni di IA “non ad alto rischio” (e dalla fissazione di alcuni criteri per operare tale distinzione) e, su questa base, identifica una serie di obiettivi disciplinari organizzati intorno ai suddetti principi, aderendo all'opzione di identificare come destinatari delle prescrizioni soltanto gli operatori economici coinvolti da applicazioni di IA ad alto rischio, e prevedendo per le altre applicazioni di IA un sistema facoltativo di “etichettatura su base volontaria”, volto ad attribuire un “marchio di qualità” a quelle applicazioni di IA non ad alto rischio che incorporino su base volontaria soluzioni tecnologiche doverose per le applicazioni di IA ad alto rischio. Il Libro Bianco si chiude con alcune linee di proposta in materia di “governance” europea in materia di IA, tendenti alla creazione di un quadro di cooperazione delle autorità nazionali competenti, al dichiarato fine di evitare la frammentazione delle responsabilità, aumentare la capacità degli Stati membri e garantire che l'Europa si doti progressivamente delle capacità necessarie per sottoporre a prova e certificare prodotti e servizi basati sull'IA.

Il Libro Bianco è aperto alla consultazione pubblica, attraverso l'invito a formulare osservazioni fino al 19 maggio 2020.

SALVATORE ORLANDO

[https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020\\_it.pdf](https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_it.pdf);

Per la consultazione pubblica: [https://ec.europa.eu/info/consultations\\_en](https://ec.europa.eu/info/consultations_en)

2020/1(6)DI

### **Intelligenza Artificiale e Costituzione francese**

Il 15 gennaio 2020 è stata depositata presso l'*Assemblée Nationale* una proposta di legge costituzionale (n. 2585) in materia di intelligenza artificiale. La proposta di legge intende inserire la “*Charte de l'intelligence artificielle et des algorithmes de 2020*” nel dettato costituzionale francese.

La *Charte* si compone di sei articoli. Il primo ne individua l'ambito applicativo. Una volta approvata la proposta 2585 e inserita la *Charte* nella Costituzione, la disciplina *in vi* contenuta

troverebbe applicazione rispetto a qualsiasi sistema che consiste di un'entità, sia fisica (come, ad esempio, un robot) sia virtuale (come, ad esempio, un algoritmo), che utilizza l'intelligenza artificiale. Per intelligenza artificiale la *Charte* intende un algoritmo che si evolve nella sua struttura, imparando rispetto alla sua scrittura iniziale. Il medesimo articolo chiarisce poi che il sistema che utilizza l'intelligenza artificiale non ha personalità giuridica e non è, quindi, idoneo ad essere titolare di posizioni giuridiche soggettive (diritti, doveri). Tale scelta segna una cesura rispetto alla famosa e discussa Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, la quale, come noto, faceva espresso riferimento alla possibilità di riconoscere la c.d. personalità elettronica per i robot autonomi più sofisticati (art. 59, lett. f). Invece di seguire quella strada, la proposta *de qua* prevede che gli obblighi derivanti dalla personalità giuridica siano a carico della persona fisica o giuridica che ospita o distribuisce il suddetto sistema che utilizza l'Intelligenza Artificiale. In questo senso, è chiarito che detta persona fisica o giuridica diverrebbe il rappresentante legale del sistema.

Il secondo articolo recepisce le c.d. leggi di Asimov sulla robotica (*Runaround*, 1942), prevedendo che un robot *i*) non possa recar danno a un essere umano né può permettere che, a causa del suo mancato intervento, un essere umano riceva danno; *ii*) debba obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non vadano in contrasto alla Prima Legge; *iii*) debba proteggere la propria esistenza, purché la salvaguardia di essa non contrasti con la Prima o con la Seconda Legge.

Il terzo articolo della *Charte* afferma invece che ciascun sistema che utilizza l'Intelligenza Artificiale sia progettato per soddisfare la piena attuazione degli articoli della Dichiarazione universale dei diritti dell'uomo (10 dicembre 1948). La subordinazione del sistema che utilizza l'Intelligenza Artificiale al rispetto dei diritti umani è ribadita all'ultima disposizione della *Charte*. Il sesto articolo, infatti, statuisce che nessuna norma prevista dalla *Charte* possa essere interpretata come giustificazione per un qualsiasi Stato, gruppo o persona di un diritto alla creazione di un sistema che utilizza l'Intelligenza Artificiale per la distruzione di uno dei diritti e delle libertà stabiliti nella *Charte*.

Il quarto articolo disciplina la nazionalità del sistema che utilizza l'Intelligenza Artificiale. Essa segue quella dell'host o del soggetto che trasmette il sistema. Il quinto articolo prevede invece come necessario l'istituzione di un meccanismo di revisione e verifica (*audit*). La frequenza di attuazione di questo meccanismo si basa sulla frequenza con cui l'algoritmo o gli algoritmi che compongono il sistema che utilizza l'intelligenza artificiale evolvono verso l'autonomia decisionale.

DANIELE IMBRUGLIA

[http://www.assemblee-nationale.fr/dyn/15/textes/l15b2585\\_proposition-loi](http://www.assemblee-nationale.fr/dyn/15/textes/l15b2585_proposition-loi)

2020/1(7)LC

### **Rome Call for AI Ethics: Per un'intelligenza artificiale umanistica**

Nell'ambito della XVI Assemblea Generale della Pontificia Accademia per la Vita (PAV), dedicata al tema dell'Intelligenza Artificiale (IA) ed alle sfide etiche da essa poste, si è tenuto a Roma il 28 febbraio 2020 il convegno “*RenAIssance, a human-centric artificial intelligence*”, che ha concluso una tre giorni di workshop sul tema “*The ‘good’ algorithm? Artificial intelligence: ethics, law, health*”.

Al termine dei lavori, il Presidente della PAV, mons. Vincenzo Paglia, ha lanciato un'iniziativa chiamata *Rome Call for AI Ethics*, in occasione della quale è stato redatto un documento inteso a sensibilizzare e veicolare, in accordo a determinati principi etici, l'azione di Governi, Organismi internazionali, *corporations*, istituzioni accademiche e ONG, rispetto allo sviluppo dell'IA. La *Rome Call for AI Ethics*, dopo aver ricordato la capitale importanza che l'IA sta progressivamente acquisendo, con una forte efficacia pervasiva, in moltissimi settori, rammenta d'altro canto i rischi che il suo incontrollato sviluppo può recare con sé, particolarmente in tre campi.

Il primo di questi è l'etica, laddove si possono inverare concrete possibilità di utilizzo dell'IA foriere di discriminazioni e destinate a restringere la dignità e la libertà degli esseri umani, soprattutto dei soggetti più vulnerabili.

Il secondo è quello educativo, che riguarda non soltanto l'accesso universale ad un elevato livello qualitativo di istruzione, fin dall'apprendimento scolastico, ma anche la necessità di ridurre quanto più possibile le disparità, al fine di dare concretezza al principio *no one left behind*.

Il terzo è l'ambito giuridico ove si ravvisa l'urgenza di codificare principi condivisi e regole chiare, a tutela tanto dell'uomo quanto dell'ambiente, ponendo al centro del dibattito pubblico la protezione dei diritti umani nell'era digitale e le nuove forme di responsabilità.

Una simile griglia etica è necessaria - si dice nella *call* - e rappresenta un valido strumento in tutte le fasi di programmazione e di utilizzo dell'IA: dalla creazione degli algoritmi alla loro applicazione pratica. Quando il prodotto è "fatto e finito" si rende necessaria l'adozione di norme per regolarne l'uso, ma il ruolo chiave dell'etica comincia sin dalle prime fasi antecedenti la sua realizzazione. Il contributo fondamentale che l'etica può dare, infatti, si riflette sui criteri che sottendono la progettazione stessa degli algoritmi e sugli stadi successivi di produzione.

La *call* si chiude con l'individuazione dei principi che devono sostenere questa *algorithmical vision*: *trasparenza, inclusione, responsabilità, imparzialità, affidabilità, sicurezza e privacy*. Tra i primi firmatari vi sono rappresentanti della PAV, di Microsoft, di IBM, della FAO, del Governo italiano (il Ministro per l'Innovazione Tecnologica e la Digitalizzazione). All'incontro ha partecipato anche il Presidente dell'Europarlamento.

LUCIO CASALINI

<http://www.academyforlife.va/content/pav/it/notizie/2020/intelligenza-artificiale-2020.html>

<http://www.academyforlife.va/content/dam/pav/documenti%20pdf/2020/CALL%2028%20febbraio/AI%20Rome%20Call%20x%20firma DEF DEF .pdf>

2020/1(8)EWDM

### **Le Linee Guide AGID del 23 marzo 2020 - Il valore giuridico della firma con il Sistema Pubblico d'identità Digitale (SPiD)**

Con la determinazione n. 157/2020 adottata il 23 marzo 2020, attraverso la quale l'Agenzia per l'Italia Digitale ("AgID") ha emanato le Linee Guida per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del codice dell'amministrazione digitale

(“CAD”), un importante tassello è stato aggiunto al processo di digitalizzazione dei documenti.

La necessità di rispondere in modo rapido ed efficace alle esigenze dei sempre più veloci traffici commerciali ha imposto l'adozione di strumenti snelli, che permettano di dare vita a negozi giuridici affidabili in termini di validità.

Le recenti Linee Guida AgID sembrano viaggiare in questa direzione.

Terminato il naturale percorso di consultazione pubblica, in un arco temporale che va dal 21 novembre al 28 novembre 2019, entreranno definitivamente in vigore il giorno successivo alla pubblicazione in Gazzetta Ufficiale di apposito avviso della predetta Determinazione 157/2020.

L'obiettivo è quello di «favorire il processo di completa digitalizzazione dei documenti».

Il CAD, all'art. 1, lett. p), offre una definizione ampia di documento informatico quale «rappresentazione informatica di atti, fatti o dati giuridicamente vincolanti», suscettibile dell'apposizione di una data opponibile ai terzi, soltanto mediante una procedura informatica di «validazione temporale» conforme alle regole tecniche.

L'entrata in vigore delle Linee Guida renderà possibile firmare atti e contratti mediante il sistema pubblico di identità digitale (c.d. SPiD), ormai sempre più diffuso tra gli operatori pubblici e privati, con il medesimo valore giuridico della firma autografa, «soddisfacendo, così, il requisito della forma scritta e producendo gli effetti di cui all'art. 2702 c.c.».

L'importante novità è data dal fatto che i cittadini, oltre alla già esistente firma elettronica qualificata, avranno a disposizione un altro strumento digitale per sottoscrivere documenti giuridicamente validi.

Le regole contenute nelle Linee Guida disciplinano le modalità tecniche «con cui i fornitori di servizi online potranno permettere agli utenti di sottoscrivere atti e contratti tramite la loro identità digitale», in conformità all'art. 20 CAD. Il capitolo tre delle medesime Linee Guida precisa che dietro l'identità digitale sia sempre presente una persona fisica.

Infatti, al fine di garantire l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio, potranno essere utilizzate esclusivamente le identità digitali della persona fisica e quelle per uso professionale, mentre non potranno essere utilizzate identità digitali SPiD per persona giuridica.

Tuttavia, la duttilità di questo strumento permetterà il suo utilizzo sia da parte dei fornitori di servizi privati sia da parte delle Pubbliche Amministrazioni e consentirà «di sostituire la firma autografa nella quasi totalità dei casi», favorendo lo sviluppo del «processo di dematerializzazione dei documenti» ormai in atto da tempo.

ETTORE WILLIAM DI MAURO

<https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/03/26/spid-emanate-linee-guida-firmare-i-documenti-online>

2020/2(1)FR

### **La Comunicazione della Commissione europea COM(2020) 66 final “Una strategia europea per i dati”**

Con la comunicazione “Una strategia europea per i dati” del 19 febbraio 2020, coeva al Libro bianco della Commissione Europea del 19 febbraio 2020 sull'Intelligenza Artificiale: “Eccellenza e Fiducia” (su cui v. la notizia [2020/1\(5\)SO](#)), la Commissione europea ha

annunciato le misure politiche e le iniziative economiche che ha in programma di promuovere e perseguire nel corso dei prossimi cinque anni, nell'ambito del progressivo sviluppo di un sistema socio-economico *data driven*.

Ne emerge un piano fortemente ambizioso, diretto a creare uno spazio unico europeo dei dati che possa imporsi a livello mondiale quale modello di riferimento per la predisposizione di un contesto favorevole alla *data economy*, in cui la regolamentazione dei criteri di utilizzo dei dati tende all'equilibrio tra l'esigenza di cogliere le innumerevoli opportunità commerciali offerte dal digitale e la nitida e irrinunciabile affermazione dei valori e dei principi fondamentali dell'ordinamento europeo.

In particolare, nelle intenzioni della Commissione, la creazione di un mercato unico dei dati poggerà su un quadro normativo che, sebbene già particolarmente solido, troverà costante ammodernamento alla luce delle nuove esigenze di regolamentazione che emergeranno a fronte del continuo progresso tecnologico, anche nell'ottica di evitare che iniziative frammentate dei singoli Stati membri possano ostacolare le misure di condivisione e sfruttamento comune dei dati in tutta l'Unione Europea. La sua realizzazione troverà inoltre compimento attraverso investimenti mirati nelle più innovative infrastrutture tecnologiche e nelle attività di ricerca e sviluppo, complessivamente dirette all'accrescimento delle competenze legate alle molteplici fasi e forme di utilizzo dei dati, nei più diversi settori dell'economia e della società.

Più precisamente, la strategia dei dati elaborata dalla Commissione individua la necessità di attuare uno schema di norme dedicato alla *governance* dei dati, a livello sia nazionale che europeo, per incentivarne l'utilizzo intersettoriale e la condivisione negli spazi comuni settoriali, per facilitarne e regolarne il riutilizzo a fini di ricerca scientifica, nonché per incoraggiare il cd. altruismo dei dati. Per la realizzazione di questi obiettivi, la Commissione intende coinvolgere soggetti pubblici e privati, favorendo una loro sempre più stretta e proficua collaborazione, in quanto il valore dei dati risiede nella possibilità di farne un utilizzo ripetuto ed innovativo. In quest'ottica, dunque, una maggiore disponibilità di dati in capo alle parti dei rapporti *business-to-business* e *business-to-government* (e viceversa), nonché tra autorità pubbliche, non potrà che tradursi nell'occasione di sfruttare al meglio le potenzialità dei dati, ad esempio permettendo loro di elaborare, rispettivamente, innovative opportunità imprenditoriali ovvero più efficaci ed efficienti politiche di erogazione dei servizi pubblici.

In secondo luogo, il documento della Commissione ne annuncia un piano di investimenti su nuovi spazi comuni europei di dati e su infrastrutture *cloud* interconnesse, oltre che sicure, potenti ed efficienti sotto il profilo energetico. Dell'istituzione di tali spazi la Commissione si fa pertanto promotrice in settori strategici e di interesse pubblico, come l'industria manifatturiera, i trasporti, l'assistenza sanitaria o i mercati finanziari, riservandosi peraltro di individuarne di nuovi. Quanto alla federazione del *cloud*, viene prospettato il programma di guidare la creazione e la regolazione di un mercato dei servizi *cloud* fondato sul rispetto dei principi di equità e trasparenza.

Con questa comunicazione possono dunque dirsi definiti i primi tratti essenziali di un vero e proprio modello europeo di gestione dei dati, in virtù del quale potremo analizzare e comprendere gli ormai prossimi interventi normativi che segneranno il futuro digitale dell'Unione Europea.

FEDERICO RUGGERI

[https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy\\_it](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_it)

2020/2(2)CR

## I lavori del 12 maggio 2020 della Commissione giuridica (JURI) del Parlamento Europeo sulla regolazione della Intelligenza Artificiale: il *Draft Report* sugli aspetti etici.

Nell'ambito del processo di regolazione dell'intelligenza artificiale (IA), lo scorso 12 maggio i membri della Commissione giuridica (JURI) del Parlamento Europeo si sono riuniti per discutere alcune proposte su diversi aspetti relativi all'IA.

In particolare, il gruppo guidato dallo spagnolo Ibán García del Blanco ha presentato il "Progetto di relazione recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle relative tecnologie (2020/2012(INL))" del 21 aprile 2020 (il "*Draft Report*"). Il *Draft Report* contiene una complessiva proposta normativa consistente in una proposta di Risoluzione del Parlamento europeo e una proposta di Regolamento del Parlamento europeo e del Consiglio, oltre a due documenti dedicati, rispettivamente, ai "principi ed obiettivi" della proposta e alla sua "motivazione"

Il *Draft Report* prende le mosse dal riconoscimento delle opportunità e dei benefici derivanti dall'IA, e quindi dalla necessità di favorirne lo sviluppo, ma, allo stesso tempo, sottolinea i rischi che tali tecnologie possono porre per la società in termini di discriminazione, esclusione dei gruppi sociali più vulnerabili e limitazione delle libertà e dei diritti fondamentali.

Ne emerge la chiara necessità di una regolamentazione di tipo etico, che si fondi cioè sul primario riconoscimento della dignità umana. Tale intervento non può che esplicarsi a livello europeo, al fine di evitare una frammentazione delle legislazioni nazionali e di garantire un livello di protezione uniforme in tutto il territorio dell'UE che rafforzi la fiducia dei cittadini europei nell'utilizzo dell'IA. Tale fiducia costituisce, infatti, la condizione necessaria per sostenere lo sviluppo e la diffusione di queste nuove tecnologie.

Il *Draft Report* individua una serie di aspetti centrali su cui il legislatore europeo è chiamato a fondare la propria normativa e che caratterizzano il testo delle allegare proposte di Risoluzione del Parlamento e di Regolamento:

- la centralità dell'intervento e della sorveglianza umani nello sviluppo, la diffusione e l'utilizzo dell'intelligenza artificiale, della robotica e delle tecnologie correlate, per cui gli operatori umani devono sempre poter ripristinare il controllo sulle tecnologie in qualsiasi momento: intelligenza artificiale "antropocentrica e antropogenica";
- la necessità di un *risk assessment* oggettivo ed imparziale al fine di valutare il livello di rischio delle tecnologie e di individuare quelle "ad alto rischio dal punto di vista del rispetto dei principi etici";
- il rispetto di rigorose misure di sicurezza, trasparenza e *accountability*;
- il rispetto della dignità umana e dell'equità di trattamento attraverso sistemi che impediscano discriminazioni fondate su pregiudizi (*bias*);
- la responsabilità sociale attraverso la salvaguardia e la promozione dei valori fondamentali della nostra società come la democrazia e la parità di genere;
- il perseguimento di obiettivi di sviluppo sostenibile, neutralità climatica ed economia circolare così da contribuire al raggiungimento degli obiettivi di sviluppo sostenibile fissati dall'ONU;

- il rispetto della normativa europea in materia di protezione dei dati personali (con particolare attenzione ai dati biometrici);
- l'istituzione di una rete di Autorità di controllo nazionali, cui affidare, *inter alia*, il compito della individuazione delle tecnologie “ad alto rischio dal punto di vista del rispetto dei principi etici”;
- l'invito alla Commissione a dar seguito alla Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), per l'istituzione di una Agenzia Europea per l'IA, e la proposta che tale Agenzia, ove istituita, sviluppi criteri comuni e una procedura per la presentazione delle domande ai fini del rilascio di un certificato europeo di conformità etica, che potrà essere richiesto da qualsiasi sviluppatore, operatore o utente che desideri certificare la valutazione positiva della conformità da parte dell'Autorità nazionale di controllo competente;
- lo sviluppo in ogni caso di standard uniformi per la valutazione di conformità ai principi etici;
- la cooperazione internazionale per garantire uno sviluppo e un utilizzo etico delle nuove tecnologie a livello globale.

Tali aspetti, riflessi nelle proposte di Risoluzione e di Regolamento, mirano a rendere l'UE un punto di riferimento per l'individuazione di un corretto bilanciamento tra tutela dei diritti dei cittadini e supporto dello sviluppo tecnologico. Secondo quanto già riportato da alcuni organi di stampa, si può prevedere che tra gli aspetti più dibattuti ci saranno la proposta di istituzione, e la delimitazione delle possibili funzioni, delle Autorità di controllo nazionali e soprattutto l'invito a dar seguito alla proposta di istituzione di una Agenzia europea per l'IA, già avanzata dal Parlamento europeo nel 2017 a mezzo della citata risoluzione.

CHIARA RAUCCIO

[https://www.europarl.europa.eu/meetdocs/2014\\_2019/plmrep/COMMITTEES/JURI/PR/2020/05-12/1203395IT.pdf](https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/PR/2020/05-12/1203395IT.pdf)

2020/2(3)SO

**(segue): il *Draft report sulla responsabilità civile***

Il “Progetto di relazione recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL))” del 27 aprile 2020 (il “**Draft Report**”) è stato discusso durante la riunione della Commissione giuridica del Parlamento europeo (JURI) del 12 maggio 2020, e presentato dal suo relatore, l'europarlamentare tedesco Axel Voss. Il *Draft Report* contiene una complessiva proposta normativa consistente in una proposta di Risoluzione del Parlamento europeo e una proposta di Regolamento del Parlamento europeo e del Consiglio, oltre a due documenti dedicati, rispettivamente, ai “principi ed obiettivi” della proposta e alla sua “motivazione”.

La proposta normativa di cui al *Draft Report*, complessivamente considerata, si caratterizza per i seguenti principali aspetti:

- Si esprime la convinzione che le nuove norme comuni per i sistemi di intelligenza artificiale (IA) dovrebbero assumere unicamente la forma di regolamento e che la

questione della responsabilità nei casi di danni o pregiudizi provocati da un sistema di IA sia uno degli aspetti essenziali da affrontare nell'ambito di tale quadro;

- Si ritiene che l'innovazione normativa in materia non debba essere totale bensì circoscritta ad alcuni profili specifici inerenti a problematiche proprie dei sistemi di IA, quali la responsabilità dell'operatore (*deployer*), la responsabilità oggettiva per i sistemi di IA “ad alto rischio” (con l'individuazione di tali sistemi e la fissazione dei relativi criteri) e l'assicurazione obbligatoria dei sistemi di IA “ad alto rischio”;
- Si ritiene, di converso, che la direttiva sulla responsabilità per danno da prodotti difettosi (direttiva 85/374/CEE) si sia dimostrata un mezzo efficace per ottenere un risarcimento per i danni cagionati da un prodotto difettoso e che pertanto essa dovrebbe essere fatta valere anche nel caso di azioni per responsabilità civile nei confronti del produttore di un sistema di IA difettoso, laddove tale sistema si qualifichi come prodotto ai sensi della suddetta direttiva, osservandosi al contempo che eventuali adeguamenti legislativi alla citata direttiva dovrebbero essere discussi in sede di riesame della stessa;
- Quanto agli specifici aspetti ritenuti bisognosi di una nuova disciplina, si esprime il convincimento che nuove norme dovrebbero essere emanate in relazione alla figura e alla responsabilità dell'operatore (“*deployer*” in lingua inglese), inteso come “la persona che decide in merito all'utilizzo del sistema di IA, esercita il controllo sul rischio associato e beneficia del suo funzionamento”, mentre l'operatore di *back-end* (“*back-end deployer*” in inglese), ossia “la persona che definisce continuamente le caratteristiche della tecnologia pertinente e fornisce sostegno di back-end essenziale e continuativo”, andrebbe assimilato, quanto ai profili di responsabilità, allo sviluppatore e al produttore quale definito dall'art. 3 della direttiva 85/374/CEE;
- In particolare, l'operatore dovrebbe generalmente rispondere secondo norme ispirate ai principi della “responsabilità per colpa”, salvo nel caso di sistemi di IA “ad alto rischio”, nel qual caso le norme attributive della responsabilità dell'operatore dovrebbero ispirarsi invece ai principi della “responsabilità oggettiva”;
- I sistemi di IA “ad alto rischio” ai fini di questa proposta di normativa sono da intendersi come quei sistemi di IA operanti in modo “autonomo” che hanno un “potenziale significativo [...] di causare danni o pregiudizi a una o più persone in modo casuale e impossibile da prevedere in anticipo”;
- La bozza di Regolamento contenuta nel *Draft Report* contiene le definizioni di “sistema di IA”, e di “autonomo”, nonché un allegato che indica 5 sistemi in tutto di IA “ad alto rischio”, di cui 3 nel settore dei trasporti (aeromobile senza equipaggio ai sensi dell'articolo 3, punto 30, del Regolamento (UE) 2018/1139; veicoli con livelli di automazione 4 e 5 ai sensi della norma SAE J3016; sistemi autonomi di gestione del traffico) e 2 nel settore della assistenza (robot autonomi; dispositivi autonomi di pulizia di luoghi pubblici);
- Viene previsto che tutti gli operatori di sistemi di IA ad “alto rischio” elencati nel predetto allegato alla bozza di Regolamento debbano obbligatoriamente dotarsi di un'assicurazione per la responsabilità civile idonea a coprire gli importi e l'entità del risarcimento previsti dal Regolamento proposto, ossia fino a 10 milioni di euro per il caso di morte o di danni alla salute o all'integrità fisica e fino a 2 milioni di euro in caso di danni al patrimonio;
- Altre disposizioni sono contenute nella bozza di Regolamento in materia di prescrizione del diritto al risarcimento dei danni cagionati da sistemi di IA ad alto

rischio (con la previsione di termini di prescrizione notevolmente lunghi da 10 a 30 anni), in materia di concorso di colpa e responsabilità solidale e di azione di regresso.

Tra i molti spunti di riflessione suscitati dal *Draft Report*, si può evidenziare come la definizione di “sistema di IA” di cui alla bozza di Regolamento, non sembra – almeno letteralmente – coerente con la definizione di “intelligenza artificiale” contenuta nella bozza di Regolamento contenuta nel coevo *Draft Report* sugli aspetti etici della IA (su cui v. *supra*, al punto precedente in questa rubrica). Può inoltre osservarsi come anche in questo contesto assuma una rilevanza centrale la scelta di individuare sistemi di IA c.d. “ad alto rischio”, similmente a quanto fatto ad altri fini nel *Draft Report* sugli aspetti etici della IA (su cui v. *supra*, al punto precedente in questa rubrica) e nel Libro bianco della Commissione Europea del 19 febbraio 2020 sull'Intelligenza Artificiale: “Eccellenza e Fiducia” (su cui v. la notizia [2020/1\(5\)SO](https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/PR/2020/05-12/1203790IT.pdf)). Quanto alle definizioni contenute nella bozza di Regolamento, sembra infine importante rilevare anche che la definizione di “danno o pregiudizio” non comprende, per espressa esclusione, i “danni morali”.

SALVATORE ORLANDO

[https://www.europarl.europa.eu/meetdocs/2014\\_2019/plmrep/COMMITTEES/JURI/PR/2020/05-12/1203790IT.pdf](https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/PR/2020/05-12/1203790IT.pdf)

2020/2(4)LC

**(segue): il *Draft report sulla proprietà intellettuale***

L'impellente necessità di delineare un quadro normativo uniforme nel campo dell'Intelligenza Artificiale, per evitare che gli Stati membri adottino approcci diversi, è sempre più avvertita dal legislatore europeo. Tale quadro deve necessariamente ricomprendere una riflessione sui diritti di proprietà intellettuale, al fine di stimolare e proteggere l'innovazione e la creatività. Per ben comprendere questa necessità, è sufficiente porre mente ad alcuni dati: le domande di brevetto registrate dall'Ufficio europeo dei brevetti relative ad invenzioni che riguardano direttamente il funzionamento dell'IA sono più che triplicate in sette anni, passando da 396 nel 2010 a 1264 nel 2017.

Così, il 12 maggio scorso, in piena emergenza sanitaria che vede gli Stati membri impegnati a traghettare i cittadini europei fuori da una crisi che si preannuncia epocale, si è tenuto un ampio dibattito, in seno alla Commissione giuridica (JURI) del Parlamento europeo, che ha preso le mosse dalle proposte di risoluzione concernenti gli aspetti relativi all'etica, alla responsabilità civile e alla proprietà intellettuale connessi all'IA.

Proprio con riferimento a quest'ultimo profilo, si è discusso attorno alla proposta di risoluzione presentata dall'europarlamentare francese Stéphane Séjourné, il quale ha chiesto di condurre una valutazione d'impatto in questo specifico settore, atteso che, nel mondo, vengono prodotte sempre più creazioni con mezzi automatizzati. La proposta di risoluzione è contenuta e commentata nel “Progetto di relazione sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza (2020/2015(INI)” del 24 aprile 2020 (il “*Draft Report*”).

A questo riguardo, l'eurodeputato ha affermato che “l'utilizzo [dell'IA] avrà implicazioni significative in particolare sulla creazione, produzione e distribuzione di beni e servizi economici e culturali”. Ed ha aggiunto che “per quanto riguarda il diritto di proprietà intellettuale, il quadro europeo deve favorire la creazione, in particolare ottimizzando l'uso

dei dati disponibili, garantendo al contempo un elevato livello di protezione per i creatori”. In questo modo ha posto un problema cruciale e di prepotente emersione perché – come afferma Séjourné – “i processi creativi sono sempre più automatizzati”. È lecito, dunque, chiedersi se: “Quindi la creazione artistica generata dall’Intelligenza Artificiale dovrebbe essere protetta o no? Io tenderei a dire che dovrebbe essere protetta”, ha concluso l’eurodeputato.

Ma la risposta a tale domanda – seppur centrale – non è destinata ad esaurire il tema. Al contrario, essa pone all’attenzione dell’interprete profili ben più complessi di disciplina su cui occorre puntare l’attenzione. Difatti, come si legge nella motivazione della proposta di risoluzione presentata da Séjourné, con il citato *Draft Report*, vengono in evidenza almeno tre aspetti.

Il primo aspetto attiene al diritto dei brevetti. Il brevetto tutela le invenzioni tecniche, vale a dire i prodotti che apportano una soluzione tecnica nuova ad un determinato problema. Pertanto, se gli algoritmi, i metodi matematici e i programmi informatici non sono brevettabili in quanto tali, possono essere integrati in un’invenzione tecnica. Per lo sviluppo dell’IA europea è essenziale che tutti gli attori economici siano consapevoli di una tale opportunità.

Il secondo concerne il diritto d’autore e il requisito di originalità che caratterizza l’opera, da ricondurre al suo autore. Ciò potrebbe costituire un ostacolo alla tutela delle creazioni generate dall’IA. Lo scopo condiviso di ogni creazione, sia essa generata dall’uomo o dall’intelligenza artificiale, rimane l’arricchimento del patrimonio culturale, anche se la creazione ha una genesi diversa. Le creazioni artistiche generate dall’IA sono sempre più numerose e si tratterebbe di ammettere, in ultima analisi, che una creazione generata dall’IA possa costituire un’opera originale, tenendo conto del risultato creativo piuttosto che del processo di creazione. Occorre, inoltre, osservare che la mancanza di protezione di questo tipo di creazioni potrebbe privare dei diritti gli interpreti, poiché la protezione del regime dei diritti connessi implica l’esistenza del diritto d’autore sull’opera interpretata.

Infine, il ruolo essenziale dei dati e della loro selezione nell’ambito dello sviluppo delle tecnologie dell’IA. Qui si pongono diversi interrogativi relativi, ad esempio, all’accessibilità di tali dati, alla dipendenza da essi, alla posizione dominante di talune imprese e, in linea generale, alla circolazione insufficiente dei dati. Occorrerà, pertanto, promuovere la condivisione dei dati generati all’interno dell’Unione Europea, quale stimolo all’innovazione in materia di intelligenza artificiale. Questa è, peraltro, l’area tematica generale individuata dalla Comunicazione della Commissione europea COM(2020) 66 final del 19 febbraio 2020, intitolata “Una strategia europea per i dati” (su cui v. la prima notizia pubblicata più sopra, [2020/2\(1\)ER](#)).

LUCIO CASALINI

[https://www.europarl.europa.eu/meetdocs/2014\\_2019/plmrep/COMMITTEES/JURI/P R/2020/05-12/1203550EN.pdf](https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/P R/2020/05-12/1203550EN.pdf)

2020/2(5)EMI

### **Le linee guida del EDPB sul consenso: chiarimenti su *cookie wall* e scorrimento dei siti web.**

Il 4 maggio 2020, il Comitato europeo per la protezione dei dati (*European Data Protection Board*, EDPB) ha pubblicato delle linee guida sul consenso alla luce del Regolamento (UE) 2016/679 (il “**Regolamento**”). Le principali novità rispetto alle linee guida in precedenza pubblicate dal *Gruppo di Lavoro Articolo 29*, riguardano la validità del consenso prestato sia mediante adesione al c.d. «*cookie wall*» sia attraverso il semplice scorrimento delle pagine online.

Innanzitutto, per «*cookie wall*» si intende la schermata che si apre all'accesso di un determinato sito, con cui si comunica l'obbligo di accettare i *cookie* per poter procedere nella navigazione online. Il problema risiede proprio nell'obbligatorietà del consenso ai fini della successiva navigazione all'interno del sito web.

In via generale, infatti, ai sensi dell'art. 4 n. 11 del Regolamento, il consenso consiste in una «manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato». Quanto al primo requisito, pertanto, il consenso non può considerarsi validamente reso laddove esso non consista in una scelta libera dell'interessato.

In proposito, alcune sentenze avevano ritenuto valido il consenso espresso dall'utente al trattamento di dati personali per finalità pubblicitarie, nonostante la condizione imposta dal sito internet che escludeva la facoltà di proseguire la navigazione senza la (a ciò) necessaria manifestazione di volontà, facendo leva sulla fungibilità del servizio offerto dal sito internet, inteso, in questo contesto, come servizio «cui l'utente possa rinunciare senza gravoso sacrificio (nella specie servizio di newsletter su tematiche legate alla finanza, al fisco, al diritto e al lavoro)» (Cass. civ. n. 17278/2018).

Questa linea interpretativa è stata, però, ampiamente contestata dalle Autorità garanti europee. Con particolare riferimento alla tematica dei *cookie*, sia l'autorità francese CNIL, con le sue linee guida del 18 luglio 2019, sia il Garante italiano della privacy, con due provvedimenti del giugno 2019, hanno sostenuto l'invalidità di un consenso assoggettato alla previa accettazione dei *cookie* ai fini dell'erogazione di uno o più servizi in rete, senza che a tal fine rilevi la fungibilità del servizio.

Per tali ragioni, il Board europeo è voluto intervenire per fare chiarezza in merito alla validità o meno del consenso prestato in tali circostanze.

Nelle linee guida dell'EDPB si sottolinea che non è in alcun modo valida la manifestazione del consenso subordinata al limite del c.d. «*cookie wall*». Non sussiste, difatti, una effettiva libertà di scelta in capo all'utente che voglia accedere a quel determinato sito web, sulla base della presunta alternatività delle piattaforme online simili.

Si chiarisce nettamente che l'utente deve poter liberamente accedere a tutte le funzionalità dei siti Internet senza la necessità di una preventiva autorizzazione da lui espressa. La preclusione che genera il c.d. «*cookie wall*» è, dunque, ritenuta incompatibile con i principi circa la manifestazione di un consenso libero, specifico ed informato (come sintetizzato chiaramente dall'esempio n. 6a del documento).

L'altra questione (già parzialmente trattata dalle linee guida del *Gruppo di Lavoro Articolo 29*) concerne la validità del consenso espresso attraverso il c.d. «*scroll*» (scorrimento) della pagina in rete. Va ricordato che secondo il Regolamento, il consenso può essere reso mediante una dichiarazione o una «azione positiva inequivocabile», cioè un'azione attiva che acconsenta al trattamento dei dati personali.

In tal senso, si afferma che il mero scorrimento all'interno di un sito web non possa essere considerato come una manifestazione di volontà chiara ed attiva da parte dell'utente. Chiarificatori, anche in questo caso, sono gli esempi nn. 15 e 16 offerti dal EDPB che escludono in via assoluta l'assimilabilità del c.d. «scroll» (o di azioni ad esso equiparabili) ad una legittima autorizzazione del soggetto interessato.

In conclusione, le linee guida qui esaminate costituiscono una valida soluzione interpretativa del Regolamento, fornendo un punto di vista opportunamente pratico, utile a tradurre correttamente i principi giuridici nell'ambito dei fenomeni della rete.

ENZO MARIA INCUTTI

[https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en)

2020/2(6)DI

### **Una nuova legge francese sui contenuti offensivi sul web**

Dopo un anno di aspre discussioni, l'*Assemblée Nationale* ha approvato la *Loi visant à lutter contre les contenus haineux sur internet* lo scorso 13 maggio. Il testo, sostenuto dal Presidente della Repubblica Macron e anche noto come *loi Avia* (dal nome della deputata che lo ha proposto), entrerà in vigore, almeno nella parte che qui interessa, a partire dal 1° luglio 2020 e si ispira alla analoga legge tedesca del 2017 (*Netzwerkdurchsetzungsgesetz*, o *NetzDG*).

La *loi Avia* modifica la legge n°2004-575 del 21 giugno 2004, (*Loi pour la confiance dans l'économie numérique*), con cui l'ordinamento francese aveva recepito la direttiva europea 2000/31/CE, e si rivolge agli *opérateurs de plateforme en ligne* come individuati all'art. L. 111-7, *Code de la Consommation* (e, quindi, ai principali social-network, motori di ricerca e siti a contenuto generato da utenti). In modo simile alla legge tedesca (*NetzDG*), anche il nuovo testo francese impone un termine breve per la rimozione del contenuto offensivo, prevedendo una sanzione elevata per il ritardo. Innanzitutto, i siti destinatari dell'obbligo hanno il dovere di predisporre un dispositivo – “*uniforme directement accessible et facile d'utilisation*” – che consenta la segnalazione del contenuto illecito. Unitamente alla predisposizione di questo dispositivo, la piattaforma deve altresì informare gli utenti delle sanzioni per le segnalazioni abusive. In secondo luogo, nelle ventiquattro ore successive alla segnalazione gli *opérateurs de plateforme en ligne* hanno l'obbligo di rimuovere o di rendere inaccessibile il contenuto che contrasta con la normativa penale in materia di incitamento alla violenza, anche sessuale o razziale, di negazione di crimini contro l'umanità. La medesima legge prevede che il termine per l'obbligo di rimozione sia più breve, un'ora, nei casi di segnalazione di contenuti illeciti perché pedopornografici o di incitamento al terrorismo. Tale dovere di rimozione obbliga il responsabile di qualunque pagina internet e non si limita, quindi, ai soli *opérateurs de plateforme en ligne*. Infine, il contenuto illecito una volta oscurato deve essere conservato in ragione di eventuali procedimenti giudiziari. Al suo posto, gli *opérateurs de plateforme en ligne* dovranno prevedere una comunicazione che ne indichi l'avvenuto ritiro. In caso di mancata o intempestiva rimozione del contenuto illecito oggetto della segnalazione, è prevista una sanzione di duecentocinquanta euro. Inoltre, la normativa ammette la possibilità di una ulteriore sanzione dall'ammontare pari al 4% del fatturato mondiale dell'anno precedente, ma non eccedente i venti milioni di euro. La decisione di questa sanzione ulteriore spetta al *Conseil supérieur de l'audiovisuel*.

Come accadde per la *NetzDG*, anche la *loi Avia* ha sollevato molte critiche e varie perplessità. Per un verso, diversi osservatori hanno criticato il meccanismo (termine breve e multa elevata), intravedendovi un rischioso incentivo alla censura. Per altro verso, da più parti si è lamentata l'assenza del coinvolgimento dell'autorità giudiziaria nella valutazione prodromica circa la decisione di rimozione di contenuti. Infine, la stessa Commissione europea aveva domandato alla Francia di non adottare il testo, intravedendovi una limitazione al mercato unico e suggerendo di attendere una risposta comune al problema del “*cyberhaine*” (C(2019) 8585).

DANIELE IMBRUGLIA

[http://www.assemblee-nationale.fr/dyn/15/dossiers/alt/lutte\\_contre\\_haine\\_internet](http://www.assemblee-nationale.fr/dyn/15/dossiers/alt/lutte_contre_haine_internet)

2020/2(7)MP

### **Il (primo) parere del Garante per la protezione dei dati personali sull'applicazione volta al tracciamento dei contagi da Covid-19.**

L'art. 6 del decreto legge 30 aprile 2020, n. 28 recante (*inter alia*) misure urgenti per l'introduzione del sistema di allerta Covid-19 (il “**Decreto**”) è stato adottato dopo l'acquisizione di un parere del Garante per la protezione dei dati personali (il “**Garante**”) reso nell'adunanza del 29 aprile 2020, intitolato “Parere sulla proposta normativa per la previsione di un'applicazione volta al tracciamento dei contagi da Covid-19” (il “**Parere**”).

Si tratta di un primo parere del Garante sulle caratteristiche della app Immuni (non menzionata né nel Parere né nel Decreto), cui dovrà però seguire una valutazione di impatto della medesima applicazione effettuata ai sensi dell'articolo 35 del Regolamento (UE) 2016/679 (il “**Regolamento**”), nonché l'adozione, da parte del Ministero della salute, sentito il Garante, di misure tecniche ed organizzative che assicurino un livello di sicurezza adeguato ai rischi per i diritti e le libertà degli interessati.

Il Garante ha in ogni caso rilevato, in questa occasione, non soltanto che la proposta normativa sottopostagli ha tenuto conto di molte delle indicazioni fornite dal Presidente del Garante nel corso di una precedente audizione tenuta in data 8 aprile 2020 presso la IX Commissione trasporti e comunicazioni della Camera dei deputati, e di quelle fornite dal Segretario generale del Garante in riscontro alle ipotesi avanzate all'interno del Gruppo di lavoro “*data-driven*” per l'emergenza Covid-19, istituito presso la Presidenza del Consiglio dei Ministri, ma soprattutto ha giudicato che la proposta normativa sottopostagli fosse conforme, per quanto rilevante, ai criteri indicati dalle Linee guida del Comitato europeo per la protezione dei dati del 21 aprile 2020 a proposito dei sistemi di *contact tracing*. Questi criteri di matrice europea possono sintetizzarsi nella necessaria volontarietà dell'adesione al sistema di tracciamento, nell'accurata previsione normativa dello stesso, nel rispetto degli obblighi di trasparenza, determinatezza ed esclusività dello scopo, di selettività e minimizzazione dei dati, di non esclusività del processo algoritmico, nella possibilità di esercitare in ogni momento i diritti di cui agli artt. 15 - 22 del Regolamento, nell'interoperabilità con altri sistemi di *contact tracing* utilizzati in Europa e nella reciprocità di anonimato tra gli utenti dell'app, i quali non devono peraltro essere identificabili dal titolare del trattamento, essendo l'identificazione ammessa al limitato fine dell'individuazione dei contagiati.

Il Garante infatti ha ritenuto che il sistema di tracciamento delineato nella proposta normativa sottopostagli sia conforme ai suddetti principi, in quanto:

a) è previsto da una norma di legge sufficientemente dettagliata quanto ad articolazione del trattamento, tipologia di dati raccolti, garanzie accordate agli interessati e temporaneità della misura;

b) si fonda sull'adesione volontaria dell'interessato, escludendo ogni forma di condizionamento della determinazione individuale e, quindi, di disparità di trattamento basate sulla scelta di consentire o meno il tracciamento;

c) è preordinato al perseguimento di fini di interesse pubblico, i quali sono indicati con sufficiente determinatezza, con esclusione del trattamento secondario dei dati raccolti per fini diversi (salva la sola possibilità - entro comunque i termini generali previsti dal Regolamento - di utilizzo, in forma anonima o aggregata, a fini statistici o di ricerca scientifica);

d) appare conforme ai principi di minimizzazione e ai criteri di *privacy by design* e *by default*, nella misura in cui prevede la raccolta dei soli dati di prossimità dei dispositivi, il loro trattamento in forma pseudonima - sempre che non sia possibile in forma del tutto anonima - escludendo il ricorso a dati di geolocalizzazione e limitandone la conservazione al tempo strettamente necessario ai fini del perseguimento dello scopo indicato, con cancellazione automatica alla scadenza del termine;

e) si conforma al principio di trasparenza nei confronti dell'interessato, garantendone la dovuta informazione;

f) ammette l'ulteriore precisazione delle caratteristiche di dettaglio del trattamento e delle misure di sicurezza adeguate da parte del Ministero della Salute: in tali sedi potranno, inoltre, essere previste le modalità di intervento umano sulla decisione algoritmica – quali *misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato* - così da soddisfare anche i requisiti di cui all'articolo 22, par. 2, lett. b) del Regolamento.

Su questa base (dopo aver suggerito alcune modifiche al testo dei commi 3 e 4 dell'articolo 6 sottopostogli: modifiche che risultano accolte nel testo Decreto), il Garante ha espresso parere favorevole sulla proposta, riservandosi in ogni caso di intervenire in futuro ai sensi dell'art. 2-*quinquiesdecies* del Codice in materia di protezione dei dati personali, ai sensi del quale, con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati ai sensi dell'articolo 35 del Regolamento, il Garante può, sulla base di quanto disposto dall'articolo 36, paragrafo 5, del medesimo Regolamento e con provvedimenti di carattere generale adottati d'ufficio, prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento (in questo caso il Ministero della Salute) è tenuto ad adottare.

MICHELA PAGANELLI

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9328050>

2020/2(8)EP

### **Stablecoin globali: prospettive regolamentari e rischi finanziari sotto la lente della BCE**

Il 5 maggio 2020, la Banca Centrale Europea (BCE) ha pubblicato, all'interno del *macroprudential bulletin*, un articolo concernente, *inter alia*, una possibile regolamentazione della funzione di gestione del risparmio assolta dagli *stablecoin* (la “**Funzione**”), al fine di porre rimedio alle attuali aporie normative (l’“**Articolo**”).

La BCE, inquadrata la natura degli *stablecoin*, quale tipologia di valuta digitale il cui valore è ancorato ad una valuta legale (e.g., dollari, euro), ha riconosciuto che gli *stablecoin* globali potrebbero coadiuvare la gestione della costante domanda di servizi di pagamento veloci, economici, e transnazionali. Al contempo, la loro proliferazione potrebbe comportare rischi sistemici di stabilità finanziaria.

L'Articolo sottolinea la difficoltà di definire quale sia il quadro normativo di riferimento della Funzione. Infatti, in base alle peculiari caratteristiche strutturali degli *stablecoin*, la Funzione può essere contemporaneamente ricompresa nel perimetro delle vigenti norme che disciplinano gli emittenti moneta elettronica, delle norme riguardanti le banche, o di quelle riguardanti i fondi di investimento.

A tal riguardo, qualora l'emittente valuta non concedesse credito, garantisca la rimborsabilità del valore nominale, e gli utenti finali avessero un credito nei suoi confronti, l'emittente potrebbe essere soggetto alla direttiva 2009/110/CE (EMD). Al contrario, ove le predette condizioni non fossero rispettate, l'emittente potrebbe essere qualificato quale istituto di deposito, soggetto al previo ottenimento di una licenza bancaria da parte della BCE.

La Funzione potrebbe, inoltre, essere ricompresa tra i fondi di investimento e soggetta alle norme contenute nella direttiva 2011/61/EU (AIFMD), o nella direttiva 2009/65/EC (UCITS), qualora gli utenti finali avessero un credito nei confronti dell'emittente, i proventi fossero investiti in attività finanziarie che non siano a rischio zero, e i detentori di valuta avessero diritto ad una quota proporzionale del valore degli asset dell'emittente. Diversamente, qualora il fondo investisse esclusivamente in strumenti finanziari con vita residua non superiore a due anni, quale fondo comune monetario, sarebbe soggetto al regolamento 2017/1131/UE (MMF).

Nell'Articolo si rileva che, a seconda di come la Funzione sia stata concepita, essa possa sfuggire alla vigente regolamentazione, potendo dare vita ad un vuoto normativo. A tal riguardo, si suggerisce di verificare se il detentore di valuta vanta o meno un credito nei confronti dell'emittente o degli asset a supporto degli *stablecoin*. In caso di risposta negativa, tale rapporto, in quanto non assimilabile a quello con un emittente, né con un fondo di investimento, sarebbe sprovvisto di regolamentazione.

L'Articolo sottolinea, inoltre, come gli *stablecoin* globali possano comportare due ordini di rischi per la stabilità del sistema finanziario: una corsa alla liquidità che abbia l'effetto di minare il funzionamento degli *stablecoin*; e la possibilità che il predetto rischio possa espandersi all'intero sistema finanziario.

In particolare, una corsa alla liquidità potrebbe essere determinata da una perdita di fiducia degli utenti finali nell'emittente o nel suo network (e.g. *cyberattack*), che porti ad improvvisi e significativi rimborsi di *stablecoin*; rimborsi che potrebbero accrescersi nell'ipotesi in cui gli utenti finali interpretassero erroneamente la detenzione di *stablecoin*, quale deposito bancario. La percezione dei predetti rischi da parte degli utenti potrebbe poi determinare effetti sistemici, il cui impatto e gravità dipenderanno dalla dimensione e interrelazione dello *stablecoin* in questione (la BCE porta l'esempio di Libra, quale *stablecoin* diffuso).

In conclusione, la BCE ritiene che i promotori di *stablecoin* debbano creare strumenti in conformità alla disciplina esistente (i.e., EMD, UCITS, AIFMD, o MMF). Altrimenti, prima che i rapporti di *stablecoin* possano essere autorizzati, sarà necessario emanare un nuovo quadro normativo, atto a prevenire i predetti rischi di stabilità finanziaria.

EUGENIO PROSPERI

[https://www.ecb.europa.eu/pub/financial-stability/macprudential-bulletin/html/ecb.mpbu202005\\_1~3e9ac10eb1.en.html](https://www.ecb.europa.eu/pub/financial-stability/macprudential-bulletin/html/ecb.mpbu202005_1~3e9ac10eb1.en.html)

2020/3(1)CR

### **La sentenza “Schrems II” del 16 luglio 2020 della Corte di Giustizia UE sul Privacy Shield con gli USA e sulle clausole contrattuali tipo.**

Il 16 luglio 2020 la Corte di Giustizia dell’Unione Europea (“CGUE”) ha pronunciato la sentenza nel caso C-311/18 sul regime di trasferimento dei dati tra l’Unione Europea e gli Stati Uniti (c.d. “**Sentenza Schrems II**”). La Corte è intervenuta su due questioni: (i) la validità della decisione 2016/1250 della Commissione europea sull’adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy (c.d. *Privacy-Shield*) e (ii) la validità della decisione 2010/87 della Commissione europea sulle clausole contrattuali tipo (“**SCCs**”).

La pronuncia segue la c.d. sentenza Schrems I del 2015 con cui, a seguito della denuncia del sig. Schrems in relazione al trasferimento dei suoi dati personali da Facebook Ireland a Facebook Inc., la CGUE aveva dichiarato invalida la decisione 2000/520 della Commissione europea che riteneva adeguato il livello di protezione garantito dal *Safe Harbour*. A seguito di tale sentenza, il sig. Schrems aveva formulato una nuova denuncia con cui chiedeva di vietare il trasferimento dei dati che Facebook Ireland continuava ad operare sulla base delle SCCs contenute nell’allegato della decisione 2010/87. Nel frattempo, la Commissione ha adottato la decisione 2016/1250 sull’adeguatezza del *Privacy-Shield*. La High Court irlandese ha quindi investito la CGUE della questione della validità di entrambe le decisioni.

Con riferimento alla decisione 2016/1250, la Corte ha evidenziato come questa riconosca il primato delle esigenze di sicurezza nazionale, interesse pubblico e rispetto della normativa statunitense. Pertanto, sulla base di tali esigenze, le autorità statunitensi sono legittimate ad accedere ai dati personali trasferiti da Paesi terzi. D’altra parte, non sono previsti limiti all’attuazione dei programmi di sorveglianza né garanzie per gli stranieri che ne siano oggetto, e non sono riconosciuti agli interessati diritti azionabili di fronte alle autorità statunitensi. Alla luce di ciò, la CGUE ha ritenuto che non sia garantito un livello di protezione equivalente a quello assicurato dal GDPR e, pertanto, ha dichiarato invalida la decisione 2016/1250.

Con riferimento alla decisione 2010/87, la Corte ha innanzitutto precisato che il livello di protezione delle SCCs deve essere valutato tenendo conto sia di quanto stabilito contrattualmente tra l’esportatore e il destinatario dei dati, sia delle garanzie previste dal sistema giuridico del Paese terzo con riferimento ad un eventuale accesso ai dati da parte delle autorità pubbliche. La Corte ha argomentato che non si possa ritenere invalida la decisione della Commissione sulla base del solo fatto che le SCCs, per la loro natura contrattuale, non vincolano le autorità di sicurezza del Paese terzo, ma è necessario stabilire se la decisione della Commissione preveda dei meccanismi che assicurino il livello di protezione richiesto e in particolare che assicurino che i trasferimenti di dati personali siano sospesi o vietati in caso di violazione delle clausole o dell’impossibilità di rispettarle. Al riguardo, la Corte ha osservato che la decisione 2010/87 ha riguardato SCCs che pongono in capo all’esportatore e al destinatario dei dati l’obbligo di verificare in via preliminare che il Paese terzo garantisca un livello di protezione adeguato, nonché l’obbligo, per il destinatario, di informare l’esportatore dell’eventuale impossibilità di rispettare le clausole con conseguente onere dell’esportatore di sospendere il trasferimento o di risolvere il contratto.

Più in particolare, la Corte ha osservato che alla stregua delle SCCs formanti oggetto della decisione 2010/87 della Commissione, il titolare del trattamento stabilito nell'Unione, il destinatario del trasferimento di dati personali, nonché l'eventuale subincaricato di quest'ultimo, si impegnano reciprocamente a far sì che il trattamento di tali dati, compreso il loro trasferimento, sia effettuato e continuerà ad essere effettuato conformemente alla «normativa sulla protezione dei dati», ossia, secondo la definizione che compare all'articolo 3, lettera f), di tale decisione, «la normativa che protegge i diritti e le libertà fondamentali del singolo, in particolare il diritto al rispetto della vita privata con riguardo al trattamento di dati personali, applicabile ai responsabili del trattamento nello Stato membro in cui è stabilito l'esportatore». E ha ulteriormente ritenuto che le disposizioni del GDPR, «lette alla luce» della Carta dei diritti fondamentali dell'Unione Europea, fanno parte di tale normativa. Alla luce di ciò, la Corte ha considerato valida la decisione in esame.

Il 17 luglio 2020 l'EDPB (*European Data Protection Board*) ha pubblicato una dichiarazione con la quale ha manifestato la sua approvazione della pronuncia della CGUE sottolineando al contempo la necessità di predisporre quanto prima nuovi strumenti e una nuova cornice per il trasferimento dei dati personali verso gli USA che sostituisca il *Privacy Shield* e garantisca il livello di protezione richiesto dal GDPR. Inoltre, il 24 luglio 2020 il medesimo *Board* ha pubblicato delle FAQ intese a fornire agli operatori i primi chiarimenti necessari per la prosecuzione del trasferimento di dati verso gli USA alla luce della pronuncia della Corte.

CHIARA RAUCCIO

Sentenza CGUE

<http://curia.europa.eu/juris/document/document.jsf?jsessionid=F88A37AF69B27E55D26CD174A97DF327?text=&docid=228677&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=15906436>

EDPB *Statement*

[https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection\\_it](https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_it)

EDPB FAQ

[https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/frequently-asked-questions-judgment-court-justice-european-union\\_en](https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/frequently-asked-questions-judgment-court-justice-european-union_en)

2020/3(2)FB

**Le conclusioni dell'Avvocato generale della Corte di Giustizia UE del 16 luglio 2020 sull'interpretazione delle direttive 2001/29/CE e 2000/31/CE sulla responsabilità dei gestori di piattaforme online con riferimento alle opere protette dal diritto d'autore.**

Il 16 luglio 2020 l'Avvocato generale della Corte di Giustizia dell'Unione europea, Henrik Saugmandsgaard Øe, ha presentato le proprie conclusioni nell'ambito delle cause riunite C-682/18 e C-683/18. Le osservazioni dell'Avvocato generale vertono sull'interpretazione dell'art. 3 della direttiva 2001/29, che riconosce agli autori di opere protette dal diritto di autore il diritto esclusivo di autorizzare o vietare qualsiasi «comunicazione al pubblico» delle medesime opere, e dell'art. 14 della direttiva 2000/31, che offre ai prestatori intermediari (cd. *hosting providers*) un esonero dalla responsabilità per le informazioni che essi memorizzano su

richiesta degli utenti al ricorrere delle condizioni ivi previste. L'indagine non è stata invece estesa alla portata del nuovo art. 17 della direttiva 2019/790, entrata in vigore solo nel corso dei procedimenti principali interessati dal giudizio sottoposto alla Corte di Giustizia (“CGUE”), e dunque non applicabile alle relative controversie. Sul punto l'Avvocato generale, andando di contrario avviso rispetto alla tesi sostenuta dal Governo francese e da una delle persone fisiche in causa (il Sig. Frank Peterson), ha dichiarato che l'art. 17 della sopravvenuta direttiva 2019/790 (che dovrà essere attuata dagli Stati membri della UE entro il 7 giugno 2021 e che richiede ai gestori di piattaforme elettroniche di ottenere una autorizzazione dai titolari dei diritti, per esempio concludendo accordi di licenza) non è rilevante nemmeno dal punto di vista ermeneutico. In particolare, l'Avvocato generale ha affermato che con l'art. 17 di tale direttiva il Legislatore europeo non ha inteso fornire “un'interpretazione retroattiva dell'articolo 3, paragrafo 1, della direttiva 2001/29 e dell'articolo 14 della direttiva 2000/31”, bensì ha “creato un nuovo regime di responsabilità per taluni intermediari online nel settore del diritto d'autore”.

L'interpretazione delle citate disposizioni è stata sollecitata dalla Corte Federale di Giustizia tedesca (Bundesgerichtshof) nell'ambito di due controversie, che possono così brevemente riassumersi:

i) nella prima (C-682/18) il Sig. Frank Peterson, produttore musicale, conveniva in giudizio la società YouTube LLC e la sua controllante Google LLC, lamentando la violazione del proprio diritto d'autore su diversi fonogrammi caricati sulla nota piattaforma YouTube da alcuni utenti senza la sua autorizzazione;

ii) nella seconda (C-683/18) la Società Elsevier Inc., gestrice dell'omonimo gruppo editoriale, conveniva in giudizio la società Cyando AG, dolendosi del caricamento sulla piattaforma di *hosting* e di condivisione di file Uploaded, gestita da Cyando, di diverse opere di cui la stessa Elsevier affermava di detenere i diritti esclusivi di sfruttamento. Anche in tale caso, le opere protette sono state messe in rete dagli utenti della piattaforma senza l'autorizzazione del titolare del diritto di privativa.

La Corte tedesca, sospendendo entrambi i giudizi, ha sottoposto alla CGUE, *inter alia*, le seguenti questioni:

1) se un gestore di una piattaforma di video su Internet come YouTube e un gestore di un servizio di condivisione di file come Uploaded, attraverso i quali gli utenti mettono a disposizione del pubblico video e file recanti contenuti protetti dal diritto d'autore senza il consenso degli aventi diritto, compiano un atto di “comunicazione” ai sensi dell'art. 3, paragrafo 1, della direttiva 2001/29;

2) in caso di risposta negativa alla prima questione, se i gestori di tali piattaforme possano beneficiare dell'esonero dalla responsabilità prevista dall'art. 14, paragrafo 1, della direttiva 2000/31;

3) se, a proposito delle informazioni che il prestatore memorizza su richiesta degli utenti del suo servizio, le condizioni alla cui ricorrenza è collegata la perdita del beneficio dell'esonero della responsabilità, consistenti, ai sensi dell'art. 14, paragrafo 1, lett. a), della direttiva 2000/31, nell'essere il prestatore “effettivamente al corrente del fatto che l'attività o l'informazione [memorizzata] è illecita” e nell'essere “al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione [memorizzata]”, debbano essere intese nel senso che tali condizioni debbono riferirsi a concrete informazioni illecite, cioè ad informazioni in particolare, o se, al contrario, sia sufficiente dimostrare che detto prestatore aveva una conoscenza o una consapevolezza generale e astratta del fatto che memorizza informazioni illecite e che i suoi servizi sono utilizzati per attività illecite;

4) se l'art. 8, paragrafo 3, della direttiva 2001/29 debba essere interpretato nel senso che la facoltà di chiedere un provvedimento inibitorio sia subordinata alla condizione di una cd.

recidiva, ossia nel senso che l'inibitoria possa chiedersi solo se, a seguito della segnalazione di una violazione, essa non sia cessata o si sia verificata nuovamente.

In risposta al primo quesito, l'Avvocato generale chiarisce in primo luogo che quando un'opera protetta è condivisa in rete su di una piattaforma come YouTube, tale opera deve senz'altro considerarsi "messa a disposizione del pubblico" ai sensi dell'art. 3, paragrafo 1, della direttiva 2001/29: ogni internauta può liberamente accedervi, nel luogo e nel momento che egli preferisca. Sicché, se difetta la preventiva autorizzazione dell'autore dell'opera, la condivisione del contenuto integra una violazione del suo "diritto esclusivo di autorizzare o vietare qualsiasi comunicazione al pubblico", previsto al citato art. 3.

Di tale violazione, però, a opinione dell'Avvocato generale, è "direttamente" responsabile solamente l'utente. Tanto perché è solamente l'utente a decidere se caricare un contenuto in rete, ovvero a decidere se trasmettere una determinata opera a un pubblico e avviare attivamente la "comunicazione"; per contro un tale ruolo – definito "imprescindibile" in richiamo alla giurisprudenza della Corte di Giustizia – non è mai ricoperto dai gestori della piattaforma online. Questi, invero, "non decidono, di propria iniziativa, di trasmettere opere a un pubblico", limitandosi a "segu[ire] le istruzioni impartite dagli utenti dei loro servizi": "Senza il loro [degli utenti, n.d.r.] intervento, i gestori delle stesse piattaforme non avrebbero nulla da trasmettere e il pubblico non potrebbe usufruire di dette opere". Essi sono cioè degli intermediari che, come previsto al considerando 27 della direttiva 2001/29, si limitano alla "mera fornitura di attrezzature fisiche" che consentono agli utenti delle loro piattaforme di realizzare la "comunicazione al pubblico" dell'opera.

Questa conclusione – precisa l'Avvocato generale – non esclude tuttavia che per i suddetti gestori di piattaforme online possa derivare una responsabilità definita "secondaria". Questione, questa, che deve essere esaminata alla luce delle norme in materia di responsabilità civile previste dagli Stati membri, nel rispetto dei limiti imposti dagli artt. 14 e 15 della direttiva 2000/31.

Quanto al secondo quesito, l'Avvocato generale suggerisce alla Corte di rispondere nel senso che il gestore di una piattaforma di condivisione di video, come YouTube, e il gestore di una piattaforma di hosting e di condivisione di file, come Uploaded, possono, in linea di principio, beneficiare dell'esonero previsto all'art. 14, paragrafo 1, della direttiva 2000/31 per qualsiasi responsabilità che possa derivare dai file che essi memorizzano su richiesta degli utenti delle loro piattaforme. A tale conclusione l'Avvocato generale giunge anzitutto constatando che, per entrambi i gestori delle piattaforme, risultano soddisfatte le due "condizioni cumulative" che circoscrivono l'ambito di applicazione dell'art. 14: i) la prestazione di un "servizio della società dell'informazione" (art. 2, lett. a) della direttiva 2000/31); ii) tale servizio "consist[e] nella memorizzazione di informazioni fornite da un destinatario del servizio [...] a richiesta" di quest'ultimo. Peraltro, viene osservato che il servizio di memorizzazione, ai fini dell'applicazione dell'art. 14, non deve necessariamente essere "l'unico oggetto" o "l'oggetto principale" dell'attività dell'intermediario: come nel caso di Google – precisa l'Avvocato generale – il servizio di "memorizzazione di informazioni" può anche essere solo "uno dei numerosi aspetti della sua attività", fermo ovviamente restando che "l'esonero previsto in tale disposizione è, in ogni caso, limitato alla responsabilità che può derivare da tali informazioni e non si estende agli altri aspetti dell'attività del prestatore in questione".

L'Avvocato generale conclude per l'applicazione dell'art. 14 anche affermando che, nei casi oggetto di scrutinio, YouTube e Cyando non svolgono alcun ruolo cd. "attivo" che conferisca loro una conoscenza o un controllo delle informazioni memorizzate. L'Avvocato generale interpreta sul punto la nota giurisprudenza della Corte di Giustizia (v. Google France e L'Oréal/eBay) osservando che, per quelle pronunce, il "ruolo attivo" del gestore della

piattaforma “si riferisce [...] al contenuto stesso delle informazioni fornite dagli utenti”: “Intendo la giurisprudenza della Corte nel senso che il prestatore svolge siffatto «ruolo attivo», tale da conferirgli «una conoscenza o un controllo» delle informazioni che memorizza su richiesta degli utenti del suo servizio, qualora non si limiti a un trattamento di tali informazioni che sia neutro per quanto riguarda il loro contenuto, ma, per la natura della sua attività, acquisisca presumibilmente il controllo intellettuale di tale contenuto. Ciò si verifica se il prestatore seleziona le informazioni memorizzate, se esso è coinvolto attivamente nel loro contenuto in altro modo oppure se presenta tali informazioni agli occhi del pubblico in modo tale da farle apparire proprie. In tali ipotesi, il prestatore esce dal ruolo di intermediario delle informazioni fornite dagli utenti del suo servizio: esso se ne appropria”. Nella specie – sempre secondo l’Avvocato generale – il ruolo “passivo” di YouTube non è escluso neppure dalla pacifica circostanza che tale piattaforma strutturi in modo particolare la presentazione dei video (inserendoli in una interfaccia di visualizzazione standard e indicizzandoli sotto varie rubriche) né dal fatto che venga fornita una funzione di ricerca e che venga effettuato un trattamento dei risultati di ricerca (anche fornendo una panoramica di “video raccomandati”). Viene osservato che controllare le condizioni di presentazione e visualizzazione dei risultati di ricerca non significa controllare “il contenuto delle informazioni ricercate”.

In merito al terzo quesito, l’Avvocato generale suggerisce alla Corte di concludere dichiarando che l’art. 14, paragrafo 1, lett. a), della direttiva 2000/31 deve essere interpretato nel senso che le ipotesi ivi previste si riferiscono, in linea di principio, a informazioni illecite concrete. Pertanto, perché un prestatore possa perdere il beneficio dell’esonero di cui all’art. 14, non sarà sufficiente dimostrare che aveva una “conoscenza” o una “consapevolezza” generale e astratta del fatto che memorizza informazioni illecite e che i suoi servizi sono utilizzati per attività illecite. Tanto – secondo l’opinione dell’Avvocato generale – lo si deduce, oltre che dall’utilizzo nello stesso dettato dell’art. 14 di articoli determinativi (“l’attività o [...] l’informazione è illecita” e “l’illegalità dell’attività o dell’informazione”), anche dal contesto generale nel quale si inserisce la disposizione. Sul punto osserva l’Avvocato generale che il Legislatore europeo ha inteso stabilire un equilibrio tra i vari interessi in gioco, da un lato espressamente escludendo un generale obbligo del prestatore di sorvegliare le informazioni trasmesse o memorizzate e di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite (art. 15 della direttiva 2000/31); d’altro lato, non appena vengano effettivamente a conoscenza di un’informazione illecita, gravando i medesimi prestatori dell’obbligo di intervenire immediatamente per rimuovere tale informazione o per disabilitarne l’accesso, nel rispetto del principio della libertà di espressione e di procedure stabilite a tal fine a livello nazionale. In tale contesto l’art. 14, paragrafo 1, della direttiva 2000/31 “è quindi destinato a costituire una base per lo sviluppo, a livello degli Stati membri, di procedure cosiddette di «notifica e rimozione» (notice and take down) e le condizioni previste alle lettere a) e b) riflettono, pertanto, la logica di tali procedure: quando un’informazione illecita concreta è portata all’attenzione di un prestatore di servizi, questi deve eliminarla immediatamente”.

Quanto all’interpretazione dell’art. 8, paragrafo 3, della direttiva 2001/29 – oggetto della quarta questione pregiudiziale – l’Avvocato generale suggerisce alla Corte di rispondere nel senso che tale articolo non richiede che si debba verificare una cd. “recidiva” per comportamento colpevole del prestatore al fine di richiedere l’intervento giudiziale.

Tanto perché, secondo l’Avvocato generale, le ingiunzioni contemplate da tale disposizione “non mirano (soltanto) a far cessare taluni comportamenti censurabili da parte loro [dei prestatori, n.d.r.]. Tale disposizione prende in considerazione anche intermediari «innocenti», nel senso che essi adempiono generalmente tutti gli obblighi loro imposti dalla

legge. Essa consente ai titolari di diritti di pretendere dagli stessi un maggiore coinvolgimento nella lotta contro le violazioni del diritto d'autore commesse dagli utenti dei loro servizi, per il fatto che essi sono generalmente i più idonei a porre fine a tali violazioni. In quest'ottica, detta disposizione consente di imporre ai medesimi intermediari nuovi obblighi mediante ingiunzioni giudiziarie. Si tratta, in definitiva, di una forma di cooperazione forzata”.

FRANCESCO BERNARDI

Conclusioni

<http://curia.europa.eu/juris/celex.jsf?celex=62018CC0682&lang1=en&type=TEXT&ancre>  
 ≡

Comunicato stampa

<https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200096en.pdf>

2020/3(3)LC

### **CasaPound vs. Facebook: il Tribunale di Roma conferma in sede di reclamo il provvedimento cautelare a favore di CasaPound.**

Con ordinanza del 29 aprile 2020, avente per oggetto il reclamo ex art. 669 *terdecies* c.p.c. avverso ordinanza resa dal Tribunale di Roma in data 11 dicembre 2019, il medesimo Tribunale, sez. XVII, ha confermato la pronuncia cautelare resa nella controversia tra CasaPound e Facebook iniziata il 9 settembre dello scorso anno, quando il noto social network procedeva alla disattivazione, senza preavviso, dell'account della Associazione di Promozione Sociale CasaPound Italia e, contestualmente, del profilo del suo dirigente nazionale ed amministratore della medesima pagina, adducendo, a motivo della disattivazione, la violazione delle condizioni d'uso, degli standard della community e, più in generale, della sua policy. In particolare, veniva richiamato «il divieto di presenza sulla piattaforma di “organizzazioni o individui che proclamano missioni violente o che sono coinvolti in azioni violente” e di diffondere messaggi di odio e discriminatori».

Ritenendo tale disattivazione illegittima, CasaPound e il suo dirigente nazionale agivano in giudizio contro Facebook, chiedendo, ex art. 700 c.p.c., un provvedimento cautelare d'urgenza per l'immediata riattivazione della pagina, indicando, relativamente al presupposto del *fumus boni iuris*, la violazione delle regole contrattuali da parte del social network e, con riferimento al *periculum in mora*, il grave pregiudizio sofferto sia in termini di danno all'immagine, determinato dalla chiusura della pagina del movimento ingiustamente accusato di diffondere odio, sia in quanto la disattivazione impediva l'esercizio di diritti fondamentali riconosciuti dalla Costituzione italiana.

Nel corso del procedimento cautelare – basato, come noto, su un giudizio sommario di cognizione e strumentale rispetto ad un successivo, ma solo eventuale, giudizio di merito – il Tribunale riteneva sussistenti entrambi i presupposti *supra* richiamati ed ordinava a Facebook Ireland Limited l'immediata riattivazione della pagina di CasaPound Italia e del profilo personale del suo amministratore. L'ordinanza muoveva dal rilievo «dell'importanza assunta da Facebook per chiunque intenda partecipare al dibattito politico e quindi per l'attuazione di principi cardine essenziali dell'ordinamento come quello del pluralismo dei partiti politici (art. 49 Cost.)». In ottemperanza a tale provvedimento, il 13.12.2019 Facebook riattivava le pagine de quibus.

Avverso codesta decisione, Facebook proponeva reclamo, respinto con l'ordinanza *de qua*, con cui il Collegio capitolino, dopo aver qualificato il rapporto tra Facebook e l'utente come un contratto atipico, nel quale il gestore fornisce gratuitamente un servizio e l'utente s'impegna a rispettare le condizioni del suo utilizzo, secondo il modello del contratto per adesione, predisposto per i clienti dalla parte fornitrice del servizio, statuiva, tra l'altro, che la disciplina del rapporto non può essere «rimessa senza limiti alla contrattazione fra le parti ed al rapporto di forza fra le stesse, né che l'esercizio dei poteri contrattuali sia insindacabile». Il ricorso al giudice per un bilanciamento degli interessi e per evitare gli abusi di diritto e di posizione della parte più “forte” sarebbe quindi necessitato, al fine di precludere «all'autonomia privata la limitazione a carico di uno dei contraenti dell'esercizio di diritti costituzionalmente garantiti», nel caso specifico la libertà di manifestazione del pensiero, protetta dall'art. 21 Cost., e la libertà di associazione, tutelata dall'art. 18 Cost.: «valori che nella gerarchia costituzionale si collocano sicuramente ad un livello superiore» rispetto alla libertà d'impresa (art. 41 Cost.) cui è riconducibile la posizione del gestore del servizio.

In conclusione, a parere dei giudici del riesame «non si ravvisano [...] elementi che consentano di concludere che CasaPound sia un'associazione illecita secondo l'ordinamento generale», stante «l'impossibilità di riconoscere ad un soggetto privato, quale Facebook Ireland, sulla base di disposizioni negoziali e quindi in virtù della disparità di forza contrattuale, poteri sostanzialmente incidenti sulla libertà di manifestazione del pensiero e di associazione, tali da eccedere i limiti che lo stesso legislatore si è dato nella norma penale»; ma precisano che «la valutazione trova il suo limite nell'oggetto del presente giudizio, la verifica della compatibilità di CasaPound con la disciplina contrattuale riguardante le condizioni di utilizzo di Facebook alla stregua dei fatti e dei documenti allegati, non competendo a questo giudice la funzione di attribuire in via generale ad una associazione una “patente” di liceità, posto che condizione e limite dell'attività di qualsiasi associazione è il rispetto della legge, la cui verifica è rimessa al controllo giurisdizionale diffuso».

LUCIO CASALINI

[https://www.corriere.it/cronache/20\\_maggio\\_29/casapound-contro-facebook-l-ordinanza-tribunale-roma-44eb8fae-a1ae-11ea-972c-41555f8ee621.shtml](https://www.corriere.it/cronache/20_maggio_29/casapound-contro-facebook-l-ordinanza-tribunale-roma-44eb8fae-a1ae-11ea-972c-41555f8ee621.shtml)

2020/3(4)FP

### **Pubblicate il 10 luglio 2020 la relazione introduttiva e le prime tre bozze di relazione del gruppo di esperti dell'*Observatory on the Online Platform Economy***

Nel più ampio panorama della strategia volta a ridisegnare il futuro digitale dell'Unione Europea (v. le notizie [2020/1\(5\)SO](#), [2020/2\(1\)FR](#), [2020/2\(2\)CR](#), [2020/2\(3\)SO](#) e [2020/2\(4\)LC](#)) la Commissione europea si è di recente fatta promotrice di una serie di iniziative che mirano allo studio e alla regolazione del settore della “*Online Platform Economy*”. In particolare, l'esigenza di conoscere più a fondo questo fenomeno in rapidissimo sviluppo e di individuarne possibili criticità ha condotto alla costituzione di un “*Observatory for the Online Platform Economy*” [C(2018), 2393 final], composto da quindici esperti indipendenti di provenienza accademica. L'osservatorio ha una funzione prevalentemente consultiva nei confronti della Commissione in relazione ai trend principali del settore, con particolare attenzione all'emergere di condotte lesive da parte delle piattaforme nell'utilizzo degli algoritmi per i processi di *decision-making* e per il *ranking*, nell'accesso e nel trattamento di dati

degli utenti e nelle relazioni *business-to-business*. Al gruppo di esperti è inoltre affidato il *follow-up* delle misure di regolazione già adottate dalla Commissione in questo settore [v., Regolamento (EU) 2019/1150 del Parlamento e del Consiglio Europeo del 20 giugno 2019 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online, P2B (*Platform-to-Business*) - Regulation].

I lavori dell'osservatorio, iniziati il 26 aprile 2018, hanno portato il 10 luglio 2020 alla pubblicazione di una relazione introduttiva e delle prime tre bozze di *progress report*, corrispondenti ai primi tre dei cinque *workstreams* individuati dall'osservatorio: (i) l'individuazione di parametri economici per dimensionare correttamente il fenomeno delle piattaforme digitali, (ii) il problema del trattamento differenziato, (iii) l'accesso e l'utilizzo da parte delle piattaforme di dati. Ad essi si aggiungeranno poi (iv) gli *online advertising* e (v) l'analisi delle problematiche relative alle piattaforme con significativo potere di mercato. I *draft progress reports* nascono al fine di preparare il terreno di dibattito con i principali *stakeholders*, in vista della pubblicazione di un unico *report* finale entro l'ultimo trimestre del 2020 sulle potenzialità ed i rischi dell'economia delle piattaforme digitali.

La relazione introduttiva alle bozze di relazione, redatta dal Presidente del gruppo di esperti per l'osservatorio, Bruno Liebhaberg, muove anzitutto da una concettualizzazione lata di "*online platform economy*", inclusiva di ogni tipo di attività derivante da transazioni commerciali effettive o potenziali realizzate nel mercato interno ed agevolate, direttamente o indirettamente, dall'uso di piattaforme online, in particolare attraverso servizi di intermediazione online e motori di ricerca. I *players* di riferimento di questo mercato - principalmente *app stores*, *social media* e motori di ricerca - operano in qualità di intermediari fra due o più parti nello scambio di beni, servizi e informazioni. Gran parte del successo conseguito dalle piattaforme digitali si giustifica, dal lato consumatori, in virtù della facilitazione nell'accesso ai servizi e al sostanziale abbattimento dei costi del prodotto finali; dal lato professionisti, nell'incentivo loro garantito nel diversificare la propria offerta commerciale e nell'ampliarla sui mercati *cross-border*. Specialmente per le PMI, dunque, le piattaforme possono rappresentare un canale esclusivo di accesso al mercato a costi iniziali particolarmente contenuti.

Tuttavia, proprio con riferimento al legame che viene ad instaurarsi tra la piattaforma e i professionisti che decidono di avvalersene al fine di promuovere la propria offerta, il gruppo di esperti rivolge un primo monito alla Commissione. La prima relazione muove difatti dall'obiettivo di mettere in luce i parametri economici sulla cui base misurare l'effettivo volume dei *market-places* digitali, come mezzo per poter stabilire il grado di dipendenza del professionista alla piattaforma. In particolare, l'osservatorio individua per il settore in esame alcuni indici rivelatori di "*economic dependancy abuse*" da parte della piattaforma, fra i quali l'imposizione al professionista di costi particolarmente elevati per uniformarsi a certi standard tecnologici, l'alta percentuale delle commissioni percepite dalla piattaforma sull'importo complessivo del servizio erogato, nonché il rilievo che la piattaforma assume nell'attenzione del consumatore rispetto al soggetto che eroga il servizio o fornisce il bene. Alla luce di questo quadro, il report si conclude con alcune raccomandazioni rivolte alla Commissione di mappare questo fenomeno con più precisione, misurandolo non tanto in termini di valore aggiunto al prodotto interno lordo, quanto al volume degli scambi realizzati sulle piattaforme e al grado di dipendenza dei professionisti nell'utilizzo di questi strumenti per garantire l'erogazione dei propri servizi ai consumatori.

L'applicazione di termini iniqui nei rapporti P2B (*Platform-to-Business*) è inoltre all'origine, secondo l'osservatorio, di potenziali discriminazioni degli utenti sulle piattaforme e di trattamenti iniqui. Gran parte delle piattaforme esistenti sul mercato svolgono un ruolo "duale", tanto da porle in una posizione di naturale conflitto di interesse: da un lato, esse

prestano un servizio neutrale di intermediazione online e di motore di ricerca, dall'altro, offrono sul mercato propri prodotti, in competizione diretta con gli utenti business. Questa prassi è tuttavia ben nota alla Commissione europea che, chiamata a decidere su un caso di discriminazione del trattamento, ha condannato Google per aver applicato ai propri motori di ricerca criteri differenti e più favorevoli per l'indicizzazione dei propri servizi di “*shopping comparison*”, rispetto ai criteri applicati ai servizi offerti da altri competitors [v. Case AT.39740 Google Search (Shopping), 27 June 2017, par. 699-700]. Il gruppo di esperti esprime inoltre preoccupazioni su talune pratiche invalse presso le piattaforme di maggiori dimensioni, volte alla realizzazione di strategie sistematiche a fini anticoncorrenziali, come l'acquisizione anticipata dei *newcomers* e il ricorrente mutamento di *policies* e condizioni negoziali. Tali condotte, oltre ad ingenerare confusione negli utenti dovuta alla mancanza di trasparenza dei servizi offerti, impongono alti costi di compliance in capo ai professionisti. Il report si conclude pertanto con l'interrogativo se le differenze che intercorrono fra i diritti municipali in ordine alla nozione di dipendenza economica non costituiscano un ostacolo alla uniforme applicazione del diritto europeo e possono dar così adito a discriminazioni nella tutela garantita a fronte di condotte abusive da parte delle piattaforme.

Il terzo ed ultimo monito rivolto da parte del gruppo di esperti riguarda l'accesso e l'utilizzo dei dati all'interno delle piattaforme digitali. I *data assets*, oltre a costituire la vera linfa vitale del funzionamento delle piattaforme, sono diventati una vera e propria moneta con la quale i consumatori pagano l'acquisto di numerosi servizi. Il *draft progress report* sui dati si concentra dunque sull'analisi e sulle diverse implicazioni del processo di acquisizione, di immagazzinamento e di utilizzo di dati da parte delle piattaforme, sul presupposto per cui gran parte degli utenti dispongono in modo particolarmente “incauto” dei dati che li riguardano, non conoscendone fino in fondo il valore effettivo. L'osservatorio muove dalle tradizionali ripartizioni dei *data assets*, per focalizzare l'attenzione su quelli di particolare rilievo per il settore della *platform economy*: informazioni che indentificano il professionista, gli effettivi ed i potenziali utenti (provenienza geografica, anagrafiche, etc.), informazioni sulle singole transazioni (prezzi, metodi di pagamento, comunicazioni interne) e sulle *performance* di ciascun professionista (volume di affari, traffico di utenti), attitudini del mercato e preferenze dei consumatori. Questi dati sono impiegati dalle piattaforme tanto in forma aggregata, quanto su base individuale. Se dal punto di vista economico è particolarmente ostico apprezzare il valore effettivo dei dati, in quanto il loro utilizzo è definibile “*non-rival*” – ossia, non preclude altri di servirsene allo stesso modo -, in ottica giuridica è nondimeno opportuno sviluppare una strategia diretta ad un'attenta *data governance*. L'osservatorio è dunque concorde nel proporre alla Commissione europea, in conclusione del proprio *report*, di evitare un approccio ai *data assets* sul modello “*one size fits all*”, ma che tenga invece conto della eterogeneità dei dati di cui le piattaforme fanno uso e della varietà di scopi professionali per i quali si dispone degli stessi.

FEDERICO PISTELLI

Relazione introduttiva e tre bozze di relazioni

<https://ec.europa.eu/digital-single-market/en/news/commission-expert-group-publishes-progress-reports-online-platform-economy>

Observatory on Online Platform Economy

<https://ec.europa.eu/digital-single-market/en/eu-observatory-online-platform-economy>

2020/3(5)EWDM

**Lo studio del luglio 2020 su “Intelligenza Artificiale e responsabilità civile” commissionato dalla Commissione JURI del Parlamento europeo.**

Dopo il “Progetto di relazione recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL))” del 27 aprile 2020 discusso durante la riunione della Commissione giuridica del Parlamento europeo (JURI) del 12 maggio 2020 (su cui v. la notizia [2020/2\(3\)SO](#)), è stato pubblicato, con data luglio 2020, uno studio sullo stesso argomento commissionato dalla medesima Commissione JURI avente come titolo *Artificial Intelligence and Civil Liability*, il cui autore è Andrea Bertolini (lo “Studio”).

Lo Studio affronta innanzitutto la questione della definizione di Intelligenza Artificiale (IA), soffermandosi sulla mancanza di una nozione generalmente condivisa e, dopo l'esame di qualche definizione “atecnica”, tratta da dizionari e opere enciclopediche, presenta una tavola di comparazione, ordinata attraverso sette criteri, avente ad oggetto 14 definizioni “tecniche” di IA (ossia definizioni intese a formare la base per una regolamentazione), 11 delle quali rese da governi nazionali, una dall'OCSE, una dall'ISO e una dal AI HLEG (il gruppo di esperti “di alto livello” sulla intelligenza artificiale, nominato dalla Commissione europea). Sulla base della predetta analisi, lo Studio suggerisce di rinunciare all'obiettivo di elaborare una definizione generale di IA, in linea con la tendenza registrata negli USA, e di proporsi piuttosto l'obiettivo di individuare modelli giuridici di responsabilità civile adeguati a specifiche applicazioni di IA. Viene sostenuto che le regole sulla responsabilità civile non possono essere unitarie, e che, in ragione delle differenze riscontrabili nelle varie applicazioni di IA, le regole sulla responsabilità debbano essere “*technology specific*” e, di conseguenza, differenziate.

Dopo aver argomentato a sostegno della tesi per cui le applicazioni basate sulla IA debbano considerarsi alla stregua di artefatti e quindi di prodotti (negando loro, di conseguenza, il riconoscimento di una soggettività o personalità giuridicamente rilevante), lo Studio ripercorre alcune questioni legate alle differenze di regime – a livello degli Stati membri della UE – tra i diversi modelli di responsabilità (contrattuale ed extracontrattuale), e si rivolge quindi alla direttiva sulla responsabilità da prodotti difettosi.

Ritiene che sia opportuno sollecitare una riforma della direttiva sulla responsabilità da prodotti difettosi che faciliti la posizione dell'utente vittima del danno, poiché l'opacità e la complessità di molte applicazioni basate sulla IA, rendono difficile, da un lato, l'individuazione del responsabile e la ripartizione della responsabilità tra più potenziali responsabili e, dall'altro, l'accertamento di un chiaro nesso di causalità tra una determinata condotta e il danno subito dalla vittima, portando a scenari di «causalità alternativa».

Tuttavia, lo Studio evidenzia come anche una riforma della direttiva sulla responsabilità da prodotti difettosi rischia di non essere sufficiente per individuare, a livello europeo, una disciplina di responsabilità delle tecnologie IA perché, nonostante il suo ambito applicativo sia teoricamente ampio, il costo e la complessità del contenzioso incentiva solo azioni di elevato valore, con il rischio di non tutelare adeguatamente gli utenti non professionisti che hanno subito danni di modico valore dal malfunzionamento della tecnologia IA. Situazioni che sicuramente cresceranno di numero con l'aumento dell'automazione nella vita di relazione.

In ogni caso, si evidenzia che se, da un lato, una revisione della direttiva sulla responsabilità da prodotto difettoso sarebbe senz'altro auspicabile, dall'altro, l'impianto della medesima – definita “*technology neutral*” – non sembra poter consentire il conseguimento di

una regolamentazione “*technology specific*”, il cui pieno raggiungimento è, di converso, ritenuto necessario dallo Studio.

Dopo aver svolto tali considerazioni, il medesimo discute quale sia l’approccio europeo consigliabile per disciplinare i problemi di conflitto presentati dalle tecnologie di IA.

In primo luogo, esprime la convinzione che il quadro normativo debba essere affidato allo strumento dei regolamenti, piuttosto che a quello delle direttive, al fine di conseguire la massima armonizzazione possibile.

In secondo luogo, argomenta a favore della opzione di politica legislativa di dedicare regole *ad hoc* solo per quelle applicazioni che danno luogo a rilevanti preoccupazioni nella società civile. Sottolinea la necessità di promuovere l’uniformità di disciplina tra gli Stati membri, attraverso riforme in materia di responsabilità civile che siano adeguate a specifiche applicazioni di IA, confermando l’idea per la quale si ritiene inefficiente la creazione di una disciplina generale e astratta data la complessità dei fenomeni considerati.

Appare pertanto opportuno, secondo lo Studio, procedere verso normative *ad hoc* che disciplinino uniformemente la responsabilità civile relativa a specifiche tecnologie basate sulla IA.

Tuttavia, tenendo sempre in considerazione i principi di proporzionalità e sussidiarietà, lo stesso ritiene che solo quelle tecnologie che danno vita a rischi importanti e presentano preoccupazioni rilevanti per la società civile dovrebbero ricevere una disciplina specifica.

Quali tipi di applicazioni debbano essere regolamentati, e in quale ordine, è questione prioritaria da definire in base allo sviluppo tecnologico e alla diffusione sul mercato delle medesime applicazioni, bilanciando gli interessi e i benefici sociali legati a essa.

Lo Studio ricorda come negli anni recenti l’UE abbia adottato determinate regole sui droni e sulle piattaforme, e suggerisce che si debba continuare su questa strada monitorando più da vicino le nuove tecnologie emergenti, eventualmente attraverso un’agenzia dedicata o un gruppo di esperti, al fine di individuare quelle tecnologie che richiedono un pronto intervento. In ogni caso, raccomanda che gli interventi normativi siano specifici e ossequiosi dei principi di proporzionalità e sussidiarietà.

Su queste basi, propone che il principio informatore utile per l’individuazione dei soggetti responsabili debba consistere nel ritenere «strettamente» responsabile la parte che è maggiormente idonea a controllare e gestire il «rischio» legato alle tecnologie di IA, aggiungendo che tale principio debba essere applicato sulla base di «classi di applicazioni» (c.d. metodo CbC: “*on a class-of-applications-by-class-of-applications basis*”), come definite dal c.d. approccio di gestione del rischio (c.d. RMA “*Risk-Management Approach*”), in linea con l’impostazione già adottata dalla direttiva sulla vendita e garanzia dei beni di consumo (direttiva 1999/44 CE).

Alla luce di quanto sostenuto, lo Studio esamina infine quattro campi di applicazione di tecnologie di IA: gli *industrial robot*, il *connected and automated driving*, le tecnologie diagnostiche dei *medical robot* e i droni.

A proposito di queste tecnologie, il medesimo trae alcune conclusioni per così dire comparative, osservando che mentre i robot industriali appaiono nel complesso regolamentati in modo adeguato – così che chi abbia subito un danno ha un evidente e facile «punto di accesso» al contenzioso – per i veicoli connessi e a guida automatizzata sembra opportuno un intervento normativo a livello europeo per semplificare il complesso scenario che emerge dalla moltiplicazione dei soggetti potenzialmente responsabili e per evitare una frammentazione di discipline tra gli Stati membri. Raccomanda uno sforzo di armonizzazione per la regolamentazione dei droni, anche se reputa un intervento in questo settore meno urgente di quello nel campo dei veicoli a guida automatizzata. Segnala la necessità di dedicare un’attenta considerazione alle applicazioni di IA per la diagnosi in campo medico, osservando

che se, da un lato, esse rappresentano una importante opportunità per migliorare l'assistenza medica, dall'altro lato l'attuale cornice regolamentare potrebbe penalizzare eccessivamente il personale sanitario. Infine, raccomanda di elaborare interventi normativi che abbiano lo scopo di proteggere i medici da eccessivi contenziosi e che introducano soluzioni alternative per risarcire le vittime, incluse forme di responsabilità di impresa.

ETTORE WILLIAM DI MAURO

[https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL\\_STU\(2020\)621926\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf)

2020/3(6)SG

### **Il Consiglio di Stato francese conferma la sanzione di 50 milioni di Euro a Google per violazione del GDPR**

Con sentenza del 19 giugno 2020, il Consiglio di Stato francese ha confermato la condanna al pagamento di 50 milioni di euro che la *Commission nationale de l'informatique et des libertés* (CNIL), ovvero l'autorità francese preposta alla tutela dei dati personali, aveva comminato alla società Google LLC con decisione del 21 gennaio 2019, per aver trattato i dati personali degli utenti in violazione delle disposizioni previste dal GDPR.

Il procedimento aveva avuto inizio su impulso delle denunce di due diverse associazioni di consumatori, *La Quadrature du Net* e *None of your business*, presentate a pochi giorni dall'entrata in vigore del GDPR.

Svolte le indagini del caso, l'Autorità francese aveva giudicato la *privacy policy* del colosso americano non sufficientemente trasparente, poiché basata su un'informativa priva delle indicazioni necessarie alla formazione di un consenso degli utenti pieno e valido sul trattamento dei loro dati.

In particolare, è stato rilevato come durante la creazione di un account Google da un telefono con sistema operativo Android, le informazioni essenziali sulla finalità del trattamento, i periodi di conservazione dei dati e le categorie di informazioni utilizzate per la personalizzazione della pubblicità, non fossero sufficientemente chiare e accessibili, poiché distribuite e frammentate su diverse pagine da aprire e in più collegamenti su cui cliccare.

Le informazioni rese da Google, peraltro, risultavano insufficienti ed eccessivamente vaghe, tanto da non consentire all'utente una piena comprensione della portata del trattamento dei suoi dati, considerati la loro raccolta e il loro massiccio utilizzo da parte dei molti servizi offerti (Google Maps, You Tube, Gmail).

Ultima ma non meno importante criticità riscontrata dall'autorità garante francese è stata la mancanza del consenso validamente espresso dall'utente al trattamento dei suoi dati personali finalizzato alla personalizzazione della pubblicità.

L'accettazione delle condizioni prospettate nell'informativa resa, infatti, veniva rilasciata attraverso una casella pre-selezionata dal sistema, insieme all'accettazione dei termini e delle condizioni d'uso del servizio. Un consenso in blocco, dunque, in violazione del Considerando 32 del GDPR, che richiede un consenso prestato mediante un atto positivo inequivocabile (quindi non attraverso caselle di default già *flaggate*), idoneo a manifestare l'intenzione libera, specifica, univoca e informata dell'interessato di accettare il trattamento dei dati personali che lo riguardano.

Alla luce delle suddette considerazioni, il CNIL ha condannato la società americana al pagamento di una sanzione di 50 milioni di Euro.

Il ricorso presentato da Google dinanzi al Consiglio di Stato francese non ha avuto gli esiti sperati dal colosso di Mountain View. L'autorità giurisdizionale, infatti, ha confermato la decisione del CNIL, ritenendo la sanzione legittima e proporzionata all'entità della violazione, dopo aver preliminarmente ritenuto sussistente la giurisdizione dell'autorità francese sulle operazioni di trattamento svolte dalla società tecnologica.

Nel ricorso, infatti, Google ha lamentato la carenza di giurisdizione del CNIL, asserendo che in ragione del fatto che la sua sede europea fosse localizzata in Irlanda, l'autorità competente dovesse essere quella irlandese.

Il Consiglio di Stato, tuttavia, ha ritenuto che quando l'autorità amministrativa francese ha avviato il procedimento, lo stabilimento irlandese non potesse qualificarsi quale stabilimento principale, in quanto esso non era coinvolto nelle operazioni di trattamento dei dati attuate nell'ambito del sistema operativo Android e dei servizi forniti da Google. Per questa ragione, i giudici francesi non hanno ritenuto applicabile il principio dello sportello unico (*one stop shop*), previsto dal GDPR, in base al quale i titolari dei trattamenti che operano in più Stati membri dell'Unione europea hanno come unico interlocutore l'autorità di controllo del paese dove hanno la sede principale.

Le decisioni delle autorità francesi hanno dato il via a un atteggiamento più rigoroso, che ha il merito di fornire un'effettiva tutela dei dati personali degli utenti digitali. Ai fini della corretta applicazione del GDPR, non potrà più ritenersi sufficiente un approccio meramente formalistico nell'elaborazione delle *privacy policy*.

Un passo importante lungo la strada - ancora tutta in salita - verso la piena consapevolezza (ancora apparentemente da acquisire) da parte dei cittadini su cosa si nasconde dietro l'utilizzo delle ormai sempre più svariate applicazioni, su quali dati vengono trattati, come, a quale fine, da chi e per quanto tempo, nonché su come questo possa incidere sui loro diritti fondamentali.

Deve anche tuttavia aggiungersi che la sanzione di 50 milioni di Euro comminata dal CNIL nel 2019 a Google risulta ad oggi un *unicum* non rilevandosi altre sanzioni precedenti e successive, minimamente comparabili nell'importo, irrogate da alcuna autorità europea per la protezione dei dati personali (compreso lo stesso CNIL), ciò che fa discutere circa l'effettivo *enforcement* delle disposizioni del GDPR in questo primo periodo di applicazione del regolamento.

SARA GARREFFA

<https://www.cnil.fr/fr/le-conseil-detat-valide-la-sanction-prononcee-lencontre-de-la-societe-google-llc>

2020/3(7)EMI

### **La «Algorithm Charter» della Nuova Zelanda.**

Il 28 luglio 2020, il governo neozelandese ha pubblicato la «Algorithm Charter» (la «Carta»), all'interno di un più ampio progetto inteso alla regolamentazione dei fenomeni connessi all'Intelligenza Artificiale. La Carta è definita come un «*evolving piece of work*», ed infatti è già stato pianificato un suo aggiornamento annuale al fine di adeguarne i contenuti alle novità legate al mondo digitale. Seppure la Carta è nata con l'obiettivo di definire standard regolatori

per l'utilizzo degli algoritmi nel settore pubblico, essa presenta aspetti interessanti generalmente per ogni settore di impiego degli algoritmi.

La *ratio* di questo provvedimento risiede nella consapevolezza di un crescente ricorso a strumenti algoritmici nell'offerta dei servizi pubblici, unitamente ad una massiccia analisi e conservazione di dati, personali e non.

Come correttamente sottolineato nel documento, gli algoritmi possono generare soluzioni improprie sulla base di una loro non corretta programmazione od ampliare gli effetti negativi delle distorsioni valutative. Infatti, se da un lato, gli algoritmi offrono prospettive nuove e mezzi particolarmente incisivi nella modulazione dei modelli di business, dall'altra, essi possono essere portatori di rischi e preoccupazioni che vanno adeguatamente affrontati.

La Carta non fornisce una definizione univoca di algoritmo ma evidenzia l'eterogeneità dei significati che si possono attribuire a questo termine. Viene richiamato, inoltre, un precedente lavoro, il «*Government Use of Artificial Intelligence in New Zealand*», in cui si compie un più specifico approfondimento delle varie tipologie di algoritmi e di strumenti tecnologici e, in particolare, degli algoritmi predittivi.

La Carta si sofferma su due obiettivi principali: trasparenza (*transparency*) e responsabilità (*accountability*) degli algoritmi. Garantire trasparenza e sicurezza nelle operazioni che utilizzano sistemi algoritmici rappresenta il principale obiettivo del documento. Si mette in risalto, infatti, che, mancando una uniformità nella gestione dei processi algoritmici, l'assenza di standard condivisi porta ad una frammentazione del quadro regolatorio e, di conseguenza, ad una rincorsa verso regole più blande.

Al momento della sottoscrizione della Carta, il governo neozelandese e le 21 autorità pubbliche aderenti hanno assunto l'impegno di rendere intellegibili le decisioni assunte dagli algoritmi, di verificare che l'analisi dei dati avvenga nel rispetto delle regole della privacy e della tutela dei diritti fondamentali e di valorizzare l'intervento umano in simili processi automatizzati, conservando una particolare attenzione verso gli aspetti etici susseguenti. L'approccio, fortemente orientato ad attribuire centralità al ruolo dell'uomo, è, dunque, sintetizzato nei punti chiave della Carta: *Transparency, Partnership, People, Data, Privacy – Ethics - Human Rights* e, infine, *Human Oversight*.

In conclusione, il documento in esame ha il merito di proporre un accurato bilanciamento degli interessi coinvolti nella ricerca del delicato equilibrio tra innovazione ed esigenze di trasparenza, tra promozione del progresso tecnologico e necessità di preservare e tutelare i fondamentali diritti dell'uomo.

Ulteriore aspetto di rilevante interesse è il coinvolgimento diretto di vari operatori del settore pubblico. La presenza di questi ultimi garantisce, infatti, una più diffusa ed immediata applicazione dei nuovi standard delineati nella Carta.

Infine, è interessante notare che la prospettiva assunta all'interno del documento persegua il virtuoso obiettivo di adattare le regole ivi esplicitate alle mutevoli dinamiche del mercato digitale, distaccandosi volutamente da granitiche definizioni e accogliendo il principio di neutralità tecnologica.

ENZO MARIA INCUTTI

<https://www.beehive.govt.nz/release/new-algorithm-charter-world-first>

2020/4(1)SG

## **La risoluzione del Parlamento europeo del 20 ottobre 2020 sul regime di responsabilità civile per l'intelligenza artificiale.**

Il dibattito europeo in materia di intelligenza artificiale (IA) prosegue nell'ambito dei lavori del Parlamento europeo, ed è da ultimo confluito in una risoluzione adottata dall'organo democratico rappresentativo dell'Unione lo scorso 20 ottobre 2020.

In attesa di una proposta legislativa da parte della Commissione europea che regolamenti il settore in maniera uniforme per tutti gli Stati membri (prevista per l'anno venturo), il Parlamento europeo ha pubblicato una risoluzione (la Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)), qui di seguito la "**Risoluzione**"), contenente una serie di raccomandazioni e indicazioni finalizzate ad indirizzare la futura disciplina della responsabilità civile applicabile al funzionamento dei sistemi di intelligenza artificiale e una proposta di regolamento.

La Risoluzione ricalca letteralmente, con alcune modifiche, il *Draft Report* in argomento discusso qualche mese fa nella Commissione JURI, ossia il Progetto di relazione recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)) del 27 aprile 2020, discusso dalla Commissione giuridica (JURI) del Parlamento europeo nella riunione del 12 maggio 2020 (il "**Draft Report**"), già illustrato su questa rubrica nella notizia [2020/2\(3\)SO](#).

I principi e gli obiettivi che permeano la Risoluzione rispondono all'avvertita esigenza di garantire da una parte la massima certezza giuridica del sistema di responsabilità di tutti i soggetti coinvolti, e dall'altra di evitare un eccesso di regolamentazione che sfoci in oneri burocratici che possano intralciare l'innovazione e il progresso di tecnologie, prodotti e servizi sviluppati da PMI o start-up.

Il giusto equilibrio tra protezione dei cittadini e incentivi alle imprese a investire nell'innovazione è lo scopo dichiarato per le nuove norme della responsabilità civile per l'IA proposte dal Parlamento europeo in questo documento, dove viene affermata anche la necessità di una piena armonizzazione che solo una fonte legislativa direttamente applicabile come il regolamento potrà garantire.

Tutte le scelte di fondo già presenti nel *Draft Report* vengono confermate nella Risoluzione, dove tuttavia vengono offerte nuove definizioni (tra cui quelle di "sistema di IA", di "autonomo" e di "alto rischio"), si introduce una distinzione tra operatore di "front-end" e operatore di "back-end", con le relative definizioni e una diversificazione di regime di responsabilità, si prevede la risarcibilità del "*danno non patrimoniale rilevante, risultante in una perdita economica verificabile*" e si riducono sensibilmente i limiti massimi degli importi dei risarcimenti.

Di conseguenza, i punti salienti della proposta di regolamento presentata nella Risoluzione (la "**Proposta di Regolamento**"), sono i seguenti:

- La Proposta di Regolamento è limitata nel suo oggetto (art. 1) alla "responsabilità civile" dei soli operatori di sistemi di IA (offrendo nell'art. 3 una definizione sia di "operatore" che di "sistemi di IA"), e dunque non riguarda la responsabilità dei produttori o di altri soggetti, per la quale la Risoluzione suggerisce una revisione della direttiva sulla responsabilità per danno da prodotti difettosi (direttiva 85/374/CEE), ed inoltre "fa salve le eventuali ulteriori azioni per responsabilità derivanti da rapporti contrattuali nonché da normative in materia di responsabilità per danno da prodotti difettosi, protezione del consumatore, anti-discriminazione,

lavoro e tutela ambientale tra l'operatore e la persona fisica o giuridica vittima di un danno o pregiudizio a causa del sistema di IA, e per il quale può essere presentato ricorso contro l'operatore a norma del diritto dell'Unione o nazionale” (art. 2 co. 3).

- Relativamente alle tipologie di danni o pregiudizi rilevanti, la responsabilità civile degli operatori di sistemi di IA di cui si occupa la Proposta di Regolamento è definita come la responsabilità derivante da “un'attività, dispositivo o processo virtuale o fisico guidato da un sistema di IA” che abbia arrecato un “danno o un pregiudizio alla vita, alla salute, all'integrità fisica di una persona fisica, al patrimonio di una persona fisica o giuridica o [...] un danno non patrimoniale rilevante risultante in una perdita economica verificabile” (art. 2 co. 1).
- La Proposta di Regolamento distingue tra “sistemi di IA ad alto rischio” (come definiti all'art. 3 ed elencati tipologicamente in via tassativa nell'allegato alla Proposta di Regolamento unitamente ai “settori fondamentali” nei quali essi vengono impiegati, e con attribuzione alla Commissione europea del potere di modificare l'elenco) ed “altri sistemi di IA”, ed istituisce due regimi di responsabilità diversi nei due ambiti (artt. 4-7 e 8-9).
- In particolare, la Proposta di Regolamento prevede per gli operatori di sistemi di IA “ad alto rischio” un regime di “responsabilità oggettiva” (tale per cui la responsabilità è esclusa solo nel caso di “forza maggiore”) un obbligo di copertura assicurativa (art. 4), termini di prescrizione del diritto al risarcimento dei danni tra i 10 anni e i 30 anni (art. 7), ed importi massimi per il risarcimento dei danni, in misura sensibilmente inferiore rispetto a quelli indicati nel precedente *Draft Report*, ossia due milioni di euro (in luogo dei dieci milioni di euro previsti dal *Draft Report*) per il caso di morte, o danni alla salute o all'integrità fisica, e un milione di euro (in luogo dei due milioni di euro previsti dal *Draft Report*) in caso di danni al patrimonio o “danni non patrimoniali rilevanti che risultino in una perdita economica verificabile”, con la specificazione che tali limiti massimi si applicano anche nel caso di danni patiti da più persone, che non potranno in quel caso ottenere importi eccedenti in totale i predetti limiti, nel senso che si tratta di limiti massimi non già per il danneggiato bensì per il responsabile o i responsabili in solido (art. 5).
- Per gli operatori degli altri sistemi di IA (ossia per i sistemi di IA non “ad alto rischio”) la Proposta di Regolamento prevede un regime di responsabilità “per colpa” comprensivo di alcune regole peculiari sulla prova a discolta a carico dell'operatore, sul danno provocato da terzi, e sull'obbligo di “cooperazione” del produttore del sistema IA nell'accertamento delle responsabilità (art. 8), nonché un rinvio “alle leggi dello Stato membro in cui si è verificato il danno o il pregiudizio” per la disciplina delle questioni relative “ai termini di prescrizione e agli importi ed entità del risarcimento” (art. 9).
- Infine, la Proposta di Regolamento, prevede alcune regole specifiche in tema di concorso di colpa, di responsabilità solidale e di azione di regresso (artt. 10, 11 e 12) senza distinguere per queste regole tra sistemi di IA ad alto rischio ed altri sistemi di IA.
- Quanto al concorso di colpa, la Proposta di Regolamento contempla, tra l'altro, la facoltà dell'operatore e della persona interessata di utilizzare i “dati generati dal sistema di IA” per l'accertamento del concorso di colpa “in conformità del

regolamento (UE) 2016/679 [GDPR] e di altre leggi pertinenti in materia di protezione dei dati” (art. 10)

- Quanto alla responsabilità solidale, la Proposta di Regolamento statuisce innanzitutto che “in presenza di più operatori di un sistema di IA, tali soggetti sono responsabili in solido”. L’art. 11 aggiunge che se un operatore di front-end è anche il produttore del sistema di IA, le disposizioni del (proposto) regolamento prevalgono su quelle della direttiva sulla responsabilità per danno da prodotti difettosi, mentre se l’operatore di back-end è anche il produttore, ai sensi dell’articolo 3 della direttiva sulla responsabilità per danno da prodotti difettosi, è opportuno che detta direttiva si applichi a tale soggetto. Ed infine si prevede che se vi è un solo operatore e tale operatore è anche il produttore del sistema di IA, le disposizioni del (proposto) regolamento dovrebbero prevalere su quelle della direttiva sulla responsabilità per danno da prodotti difettosi.
- Quanto infine all’azione di regresso, l’art. 12 prevede sia un diritto di regresso tra operatori solidalmente responsabili (stabilendosi, tra l’altro, che le quote interne di responsabilità debbano asseverarsi sulla base dei “rispettivi gradi di controllo che gli operatori hanno esercitato sul rischio connesso all’operatività e al funzionamento del sistema di IA. Se non è possibile ottenere da un operatore responsabile in solido il contributo che gli è attribuibile, tale importo mancante è a carico degli altri operatori”) sia un diritto di regresso dell’operatore nei confronti del produttore di un sistema di IA difettoso (prevedendosi che tale diritto debba esercitarsi conformemente alla direttiva 85/374/CEE e alle disposizioni nazionali che disciplinano la responsabilità per danno da prodotti difettosi).

SARA GARREFFA

[https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276\\_IT.html](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_IT.html)

2020/4(2)MS

### **La proposta della Commissione europea del 24 settembre 2020 avente ad oggetto l’emanazione di un Regolamento Europeo sui Mercati di Cripto-attività.**

Il 24 settembre 2020, la Commissione europea ha pubblicato un “pacchetto per la finanza digitale” volto ad incentivare lo sviluppo di un mercato unico digitale innovativo per i finanziamenti. *La ratio* di fondo è che la creazione di tale mercato apporterà “benefici per i cittadini europei e sarà fondamentale per la ripresa economica dell’Europa, offrendo prodotti finanziari migliori per i consumatori e aprendo nuovi canali di finanziamento per le imprese”. Il pacchetto si presenta ampio e articolato, occupandosi di definire gli orizzonti strategici per la “finanza digitale”, nonché di delineare proposte legislative in materia di “cripto-attività” e di “resilienza digitale”. Si tratta di un’iniziativa che ben esemplifica l’approccio olistico della Commissione europea durante i lavori preparatori: le proposte si inquadrano nel Piano d’Azione definito nel 2018, muovono dagli studi in materia del Parlamento europeo e delle Autorità europee di vigilanza e sono state precedute da una consultazione degli *stakeholders* lanciata nella primavera del 2020.

Tra le proposte, quella avente ad oggetto l’emanazione di un regolamento europeo sui Mercati di Cripto-attività (*Proposal for a regulation of the european parliament and of the council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 - COM(2020) 593 final-*

2020/0265(COD) – “**Proposta MiCAR**”), mira a dotare l’Unione Europea di norme uniformi in materia di emittenti di cripto-attività, nonché di prestatori di servizi in cripto-attività (art. 2, comma 1, MiCAR), superando così l’attuale frammentazione tra regimi nazionali. L’importanza di assicurare agli operatori del settore la possibilità di avvalersi di un passaporto europeo per offrire i propri prodotti e servizi su cripto-attività nel territorio dell’Unione è ribadita a più riprese nei considerando (cfr. in particolare considerando 4 e 5) e giustifica, del resto, la stessa scelta di intervenire nella forma giuridica del regolamento. L’ampiezza delle misure elaborate dalla Commissione si lega anche alla presenza, a fianco della Proposta MiCAR, di due proposte satellite: la prima volta ad introdurre alcuni adattamenti alle disposizioni vigenti in materia di infrastrutture di mercato con particolare riferimento ad infrastrutture basate su tecnologie a registri distribuiti (*Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology - COM/2020/594 final*); la seconda volta a coordinare l’attuale disciplina finanziaria europea con le novità contenute nel “pacchetto per la finanza digitale” (*Proposal For A Directive Of The European Parliament And Of The Council Amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341- COM/2020/596 final*).

La proposta MiCAR si articola in sette titoli e può essere concettualmente suddivisa in quattro parti. La prima (coincidente con il Titolo I) è dedicata alle definizioni e alla individuazione del campo di applicazione del Regolamento. La seconda (coincidente con i Titoli II, III e IV) si occupa dell’offerta di cripto-attività, declinando la disciplina a seconda dell’oggetto di emissione. La terza (coincidente con il Titolo V) riguarda i prestatori di servizi in cripto-attività, mentre la quarta (coincidente con i Titoli VI e VII) guarda alla prevenzione e alla repressione degli abusi di mercato, nonché ai poteri e ai rapporti tra Autorità competenti.

La lettura del Titolo I lascia trasparire la forte influenza che gli studi elaborati dalle Autorità di vigilanza – e specialmente il parere reso dall’ESMA alla Commissione nel gennaio 2019 – hanno avuto nella definizione e classificazione delle cripto-attività. La proposta offre una definizione estremamente ampia di cripto-attività che, nell’accogliere i suggerimenti elaborati dalla *Financial Action Task Force*, ricomprende ogni “*rappresentazione digitale di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga*”. Tuttavia, il fatto che una certa attività sia attratta in questa definizione non è di per sé sufficiente ad individuare la disciplina applicabile. Da un lato, infatti, restano al di fuori del MiCAR le cripto-attività che già rientrano nella definizione di strumenti finanziari, moneta elettronica, depositi, depositi strutturati o cartolarizzazioni (art. 2, comma 2). Dall’altro lato, il MiCAR calibra la disciplina a seconda che la cripto-attività si qualifichi alla stregua di *utility token*, token collegato ad attività o token di moneta elettronica, offrendo una definizione (puramente descrittiva) di ciascuno di questi. Sia i token collegati ad attività che quelli di moneta elettronica sono riconducibili alla famiglia delle cc.dd. *stablecoin*, in quanto idonei a mantenere un valore stabile facendo riferimento, nel primo caso, al valore di diverse monete fiduciarie aventi corso legale, di una o più merci o di una o più cripto-attività, oppure di una combinazione di tali attività, nel secondo caso, al valore di una moneta fiduciaria avente corso legale. Infine, sotto il profilo soggettivo, il MiCAR contempla ipotesi di esenzione sia totale che parziale legate alla particolare natura dei soggetti interessati (art. 2, commi 3-6).

La seconda parte della Proposta MiCAR è dedicata, come detto, all’offerta di cripto-attività. Le previsioni in larga parte recepiscono pratiche di mercato consolidate nel tempo (tra tutte, quella relativa alla pubblicazione dei cc.dd. *white paper*) e riadattano al mercato delle cripto-attività norme già radicate nella disciplina europea del mercato dei capitali (in

particolare, quelle contenute nel Regolamento (UE) 2017/1129 relativo al prospetto da pubblicare per l'offerta pubblica o l'ammissione alla negoziazione di titoli in un mercato regolamentato). L'offerta di cripto-attività deve, infatti, accompagnarsi alla pubblicazione di un documento informativo e al rispetto di taluni obblighi di condotta, tra i quali rientra un "obbligo di sicurezza informatica", su cui le ESAs sono chiamate ad emanare standard tecnici. A differenza di quanto previsto per le IPOs, il *white paper* è soggetto alla previa autorizzazione dell'Autorità competente soltanto nelle ipotesi in cui oggetto di offerta siano token collegati ad attività, atteso il rischio che queste attività potrebbero porre per la stessa sovranità monetaria. Quanto ai token di moneta elettronica – e stante la loro espressa equiparazione alla moneta elettronica – l'offerta può essere condotta unicamente da istituti di credito o istituti di moneta elettronica. È, peraltro, intuitivo che la necessità di individuare un soggetto emittente esclude che questa disciplina possa applicarsi a Bitcoin o alle altre cripto-valute prive di un emittente.

Spostando l'attenzione sulle norme che disciplinano i prestatori di servizi in cripto-attività, è chiara ancora una volta l'influenza esercitata della disciplina del mercato dei capitali, ed in particolare dalla disciplina MiFID. In primo luogo, la proposta MiCAR affianca ai servizi di custodia, di gestione di piattaforme di negoziazione e di scambio di cripto-attività – già ampiamente diffusi sul mercato – i tradizionali servizi finanziari elencati dalla MiFID: esecuzione di ordini, collocamento, ricezione e trasmissione di ordini, e consulenza sugli investimenti. La Proposta richiede poi che coloro che intendono operare come fornitori di servizi siano autorizzati dall'Autorità competente e rispondano a requisiti prudenziali, organizzativi e a regole di condotta che rispecchiano quelle già previste nei vari *silos* della regolamentazione dell'Unione. Spiccano, in particolare, gli obblighi di agire "*in modo onesto, corretto e professionale secondo il migliore interesse dei [...] clienti effettivi e potenziali*", di fornire ai clienti "*informazioni corrette, chiare e non fuorvianti*" e di mantenere e applicare "*una politica efficace per prevenire, individuare, gestire e comunicare i conflitti di interesse*".

Infine, con riguardo ai Titoli VI e VII, la Proposta mira anzitutto a prevenire e reprimere i potenziali abusi di mercato in relazione alla negoziazione di cripto-attività. Anche in questo caso, è forte l'influenza esercitata dall'assetto normativo delineato dal Regolamento 596/2014 sugli abusi di mercato: sono, infatti, previsti l'obbligo dell'emittente di rendere pubbliche le informazioni privilegiate, il divieto di *insider trading*, il divieto di diffondere illecitamente informazioni privilegiate, nonché quello di porre in essere attività che possano tradursi in una manipolazione del mercato.

Quanto alla disciplina sulla vigilanza, ogni Stato membro è libero di designare le autorità competenti per lo svolgimento dei compiti delineati dalla Proposta. Specifiche competenze sono poi attribuite all'EBA in relazione alla vigilanza sui token collegati ad attività e quelli di moneta elettronica cc.dd. significativi.

MARTINA SCOPSI

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>

2020/4(3)MP

**La prima sentenza della Corte di Giustizia UE sul principio di «neutralità di Internet» ai sensi del regolamento (UE) 2015/2120.**

Con sentenza del 15 settembre 2020 nelle Cause riunite C-807/18 e C-39/19 (la “**Sentenza**”), la Corte di Giustizia UE ha per la prima volta offerto un’interpretazione sul principio di accesso a un’Internet aperta, detto anche di neutralità della rete, in particolare in relazione alle disposizioni di cui ai primi tre paragrafi dell’art. 3 del regolamento (UE) 2015/2120 del Parlamento europeo e del Consiglio del 25 novembre 2015 che stabilisce misure riguardanti l’accesso a un’Internet aperta e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all’interno dell’Unione (il “**Regolamento**”).

La Corte di Giustizia ha chiarito che le disposizioni di cui ai primi tre paragrafi dell’art. 3 del Regolamento ostano, per motivi diversi, a che un fornitore di servizi di accesso a Internet privilegi talune applicazioni e taluni servizi, mediante pacchetti facenti parte di accordi contrattuali che permettano a tali applicazioni e servizi di beneficiare di una «tariffa zero» che ne consenta una fruizione sostanzialmente illimitata, assoggettando al contempo l’utilizzo delle altre applicazioni e degli altri servizi disponibili a misure di blocco e/o di rallentamento del traffico.

La pronuncia ha preso le mosse da alcune soluzioni di abbonamento offerte della società ungherese Telenor, fornitrice di servizi di accesso a Internet, denominate ‘MyChat’ e ‘MyMusic’, consistenti in pacchetti di accesso preferenziale, contemplanti una c.d. «tariffa zero» per l’utilizzo di determinati applicazioni e servizi, in particolare consistenti in sei applicazioni specifiche di comunicazione on-line nel caso del pacchetto ‘MyChat’ (Facebook, Facebook Messenger, Instagram, Twitter, Wiber e Whatsapp) e in quattro applicazioni per la trasmissione di musica (Apple Music, Deezer, Spotify e Tidal) e sei servizi radiofonici nel caso del pacchetto ‘MyMusic’. Le offerte in questione prevedevano che non si computasse il traffico dei dati interessati dalla «tariffa zero» nel monte dati complessivo acquistato dai clienti, consentendo inoltre ai clienti, dopo l’esaurimento del volume di dati acquistati, di continuare a utilizzare senza restrizioni tali servizi e tali applicazioni specifici, mentre alle altre applicazioni e agli altri servizi disponibili venivano applicate misure di rallentamento del traffico (nel caso di ‘MyChat’) e di rallentamento e blocco del traffico (nel caso di ‘MyMusic’).

L’Ufficio nazionale dei media e delle comunicazioni ungherese (“**UNMC**”) adottava due decisioni con le quali dichiarava che tali due pacchetti attuavano misure di gestione del traffico che non rispettavano l’obbligo generale di trattamento equo e non discriminatorio del traffico Internet ai sensi dell’articolo 3, paragrafo 3 del Regolamento, ordinando alla società Telenor di porvi fine.

Dopo la conferma di tali provvedimenti da parte del Presidente dell’UNMC, Telenor faceva ricorso alla Corte di Budapest Capitale, lamentando, in sostanza, che l’UNMC aveva errato nell’applicare al caso di specie l’art. 3 paragrafo 3 del Regolamento, in quanto tale disposizione, sancendo un obbligo generale di trattamento equo e non discriminatorio del traffico nella fornitura di servizi di accesso a Internet, riguarderebbe unicamente le misure di gestione del traffico attuate unilateralmente dai fornitori di servizi di accesso ad Internet, e non si applicherebbe ai casi, come quello relativo ai pacchetti ‘MyChat’ e ‘MyMusic’, facenti parte di accordi conclusi con clienti, che, come tali, possono rientrare solo nell’ambito di applicazione del paragrafo 2 dell’art. 3 del Regolamento, che vieta ai fornitori dei servizi di accesso ad Internet di concludere accordi o adottare pratiche commerciali limitativi

dell'esercizio dei diritti degli utenti finali come previsti dal paragrafo 1 dell'art. 3 del Regolamento.

La Corte di Budapest Capitale, così adita, interpellava quindi la Corte di Giustizia UE in via pregiudiziale in merito all'interpretazione dei paragrafi 1, 2 e 3 dell'articolo 3 del Regolamento in relazione ai vari profili di giudizio sottoposti alla sua cognizione.

La Corte di Giustizia UE ha innanzitutto dichiarato nella Sentenza che la disposizione di cui al paragrafo 2 dell'art. 3 del Regolamento va interpretata alla luce del Considerando 7 del Regolamento, avendo cioè riguardo alle posizioni di mercato dei fornitori dei servizi di accesso a Internet e dei fornitori dei contenuti, così che si possa stabilire la "portata" degli accordi e delle pratiche commerciali ivi menzionate, e in particolare la loro idoneità a limitare significativamente la scelta degli utenti finali e così i diritti menzionati nel paragrafo 1. Su questa base, la Corte di Giustizia ha rilevato che la conclusione di accordi mediante i quali determinati clienti sottoscrivono abbonamenti che combinano una «tariffa zero» con misure di blocco o di rallentamento del traffico connesso all'utilizzo di servizi e di applicazioni diversi da quelli che beneficiano di tale «tariffa zero» è idonea a limitare l'esercizio dei diritti degli utenti finali, ai sensi del paragrafo 2 dell'articolo 3 del Regolamento, in combinato disposto con il paragrafo 1 dello stesso articolo. Ciò in quanto, se simili accordi sono conclusi su una parte significativa del mercato, siffatti pacchetti sono tali da incrementare l'utilizzo delle applicazioni e dei servizi privilegiati e, correlativamente, da rarefare l'utilizzo delle altre applicazioni e degli altri servizi disponibili, che è reso tecnicamente più difficoltoso, se non impossibile. Nella Sentenza viene argomentato che quanto più il numero di clienti che concludono simili accordi è rilevante, tanto più l'impatto cumulativo di tali accordi può, tenuto conto della loro portata, comportare una notevole limitazione all'esercizio dei diritti degli utenti finali, o addirittura compromettere l'essenza stessa di tali diritti.

Per quanto riguarda l'interpretazione del paragrafo 3 dell'art. 3 del Regolamento, la Corte ha rilevato, innanzitutto, che esso contiene un obbligo generale di trattamento equo, senza discriminazioni, restrizioni o interferenze del traffico al quale non si può derogare nemmeno attraverso accordi conclusi dai fornitori di servizi di accesso a Internet con gli utenti finali, o attraverso pratiche commerciali adottate da tali fornitori, con ciò implicitamente rispondendo all'obiezione di Telenor che riteneva invece non applicabile il paragrafo 3 dell'art. 3 del Regolamento ai pacchetti 'MyChat' e 'MyMusic', in quanto facenti parte di accordi conclusi con clienti (e come tali, secondo Telenor, soltanto assoggettabili al paragrafo 2 dell'art. 3 del Regolamento). In secondo luogo, la Corte ha chiarito che il sindacato di cui al paragrafo 3 dell'art. 3 del Regolamento è indipendente da quello di cui al paragrafo 2 del medesimo articolo. In terzo luogo, la Corte ha dichiarato che quando misure di rallentamento o di blocco del traffico sono basate non su requisiti di qualità tecnica del servizio, ma su considerazioni di ordine commerciale, tali misure devono ritenersi incompatibili con il paragrafo 3 dell'art. 3 del Regolamento, in quanto discriminatorie.

In conclusione, relativamente alle questioni sottoposte al controllo del giudice del rinvio, con la Sentenza la Corte di Giustizia UE ha ravvisato una violazione sia del paragrafo 2, in combinato disposto con il paragrafo 1, dell'art. 3 del Regolamento, in quanto i detti pacchetti, i detti accordi e le dette misure di blocco del traffico limitano l'esercizio dei diritti degli utenti finali come previsti dal paragrafo 1 del medesimo articolo; sia del paragrafo 3 dell'art. 3 del Regolamento, in quanto le dette misure di blocco o di rallentamento sono basate su considerazioni di ordine commerciale.

MICHELA PAGANELLI

<http://curia.europa.eu/juris/document/document.jsf?jsessionid=5ED4CD6277132D7FE E048CCA296A9D92?text=&docid=231042&pageIndex=0&doclang=it&mode=req&dir=&occ=first&part=1&cid=17593535>

2020/4(4)CM

**La lunga marcia verso il *GDPR* cinese: la prima legge sulla protezione delle informazioni personali della Repubblica popolare nella bozza per i commenti pubblici del 21 ottobre 2020.**

Il 21 ottobre 2020, l'Assemblea nazionale popolare (全国人民代表大会, *Quangguo Renmin Daibiao Dabui*), principale organo legislativo cinese, ha presentato la bozza della 'Legge sulla protezione dei dati personali' (个人信息保护法, *geren xinxi baohu fa*), al fine di sottoporla alla consultazione pubblica. Essa è la prima normativa organica e sistematica in materia di protezione delle informazioni personali della repubblica popolare. Ad oggi, lo statuto delle informazioni personali, in Cina, è frammentato in una serie di leggi susseguitesi nel tempo (vedi il Capitolo IV della 'Legge sulla sicurezza informatica' del 2016, l'articolo 111 dei 'Principi generali del diritto civile' del 2017, gli articoli 5, 23, 25, 32, 79 e 87 della 'Legge sul commercio elettronico' del 2019, gli articoli 31 e 40 della 'Legge sulla crittografia' del 2019, il Capitolo VI della Parte IV del 'Codice civile' promulgato nel 2020) e in una fonte di rango secondario (mi riferisco allo *Standard GB/T 35273-2020 on Information Security Technology - Personal Information Security Specification*).

La bozza è composta da settanta articoli suddivisi a loro volta in otto capitoli: (a) disposizioni generali; (b) regole per il trattamento delle informazioni personali; (c) regole per il trasferimento transfrontaliero delle informazioni personali; (d) diritti delle persone nelle attività di trattamento delle informazioni personali; (e) doveri dei soggetti che trattano le informazioni personali; (f) dipartimenti che adempiono i doveri e le responsabilità in materia di protezione dei dati personali; (g) responsabilità legale; (h) disposizioni supplementari.

Dopo aver chiarito in premessa lo scopo della legge, se ne definisce l'ambito di applicazione, circoscritto a tutte quelle attività di trattamento delle informazioni personali compiute da organizzazioni e individui nell'esercizio della propria attività d'impresa, all'interno del territorio della Repubblica Popolare cinese, ed escludendola per tutti quei trattamenti effettuati nell'ambito di attività a carattere esclusivamente personale o domestico (similmente a quanto previsto nel *GDPR*).

Si distinguono le informazioni in *personali* (个人信息, *geren xinxi*: 'vari tipi di informazioni elettroniche o in altro modo registrate relative a un soggetto identificato o identificabile', Articolo 4) e in *personali sensibili* (敏感个人信息, *mingan geren xinxi*: 'informazioni personali la cui fuga o uso illecito comporterebbe un trattamento discriminatorio o gravi danni alla sicurezza personale o dei propri beni, inclusa la razza, l'etnia, le credenze religiose, i dati biometrici, le informazioni mediche relative alla salute, i conti finanziari e la posizione personale', Articolo 29). La prima definizione ricalca quasi interamente quella contenuta nella 'Legge sulla sicurezza informatica', all'articolo 76, e nel *GDPR* europeo, all'articolo 4, mentre la seconda costituisce una specificità del sistema cinese.

La legge sembrerebbe mutuare alcuni principi che sono già sanciti nel *GDPR*: in ossequio dei quali i dati dovranno essere trattati in modo legale e legittimo, per un chiaro e ragionevole scopo, per un tempo determinato e secondo il crisma della buona fede. Essa impone ai

soggetti che trattano informazioni personali gravosi oneri al fine di perseguire un sano sviluppo della *digital economy*, pena l'imposizione di sanzioni.

È evidente l'intento del legislatore cinese di contemperare due opposti interessi: da un lato, la promozione dell'innovazione attraverso lo sfruttamento dei dati, dall'altro, l'esigenza di tutelare l'interesse personale degli individui. È necessario infine precisare che il progetto, prima di essere approvato, necessita di almeno altre tre revisioni, durante le quali potrebbe chiaramente subire delle modifiche, seppur minime.

CORRADO MORICONI 马思勇

[https://www.dataguidance.com/sites/default/files/china\\_draft\\_personal\\_data\\_law.pdf](https://www.dataguidance.com/sites/default/files/china_draft_personal_data_law.pdf)

[http://www.ahwx.gov.cn/zcfg/gfxwj/202007/t20200708\\_4629245.html](http://www.ahwx.gov.cn/zcfg/gfxwj/202007/t20200708_4629245.html)

[https://www.sohu.com/a/426584424\\_780954](https://www.sohu.com/a/426584424_780954)

2020/4(5)CR

### **Le FAQ del Garante per la protezione dei dati personali sulla refertazione online.**

Lo scorso ottobre il Garante privacy è intervenuto pubblicando dei chiarimenti, sotto forma di FAQ, sul tema della refertazione online. Si tratta di un tema di estrema rilevanza data la natura particolarmente sensibile dei dati coinvolti quali sono, appunto, i dati sanitari. Le nuove FAQ intervengono ad aggiornare, per la prima volta dopo l'entrata in vigore del GDPR, le precedenti "Linee guida in tema di referti online" del 2009.

Innanzitutto, il Garante precisa che per "referto online" deve intendersi la possibilità di accedere ad un referto medico tramite modalità digitali quali il Fascicolo sanitario elettronico, siti web, posta elettronica anche certificata.

Relativamente alla base giuridica, il Garante, confermando quanto già dichiarato nel DPCM dell'8 agosto 2013, specifica che il trattamento deve essere fondato sul consenso esplicito, libero, specifico e informato dell'interessato, preceduto dal rilascio di un'apposita informativa ex artt. 13-14 GDPR, distinta rispetto a quella relativa al trattamento dei dati personali per finalità di cura, che indichi le caratteristiche del servizio di refertazione online. Il consenso, dunque, continua a porsi come base giuridica necessaria, diversamente da quanto accade per il trattamento dei dati necessario all'erogazione della prestazione sanitaria ex art. 9, par. 2, lett. h) GDPR, in quanto la refertazione online costituisce un servizio accessorio, ulteriore e distinto dall'attività di cura, di cui l'interessato può liberamente scegliere se avvalersi o meno, senza che questo pregiudichi il suo diritto all'erogazione della prestazione sanitaria. Il consenso, inoltre, può essere concesso con riferimento ad alcuni referti ma escluso per altri (fermo restando il divieto di refertazione online per accertamenti relativi ad indagini genetiche o all'HIV).

Al fine di assicurare un'adeguata tutela dei dati sensibili contenuti nel referto, il Garante individua una serie di misure di sicurezza di natura sia tecnica che organizzativa che la struttura sanitaria deve porre in essere. Con specifico riferimento alla comunicazione del referto al paziente, devono essere adottati protocolli di comunicazione sicuri (*https*) e sistemi di autenticazione forte dell'interessato (*strong authentication*); il referto deve essere reso disponibile sul sito web della struttura per un massimo di 45 gg. con possibilità per l'interessato di cancellare dal sistema di consultazione tutti o alcuni dei referti che lo riguardano. In caso di trasmissione tramite e-mail, il referto deve essere spedito come allegato e non deve comparire come testo nel corpo del messaggio; il file contenente il referto deve

essere protetto tramite password e eventuali SMS possono essere utilizzati solo per dare notizia della disponibilità del referto senza riportare la tipologia di accertamenti effettuati, il loro esito o le credenziali di autenticazione dell'interessato. A queste si aggiungono le specifiche misure di sicurezza già previste dalle Linee guida del 2009 e dal DPCM del 2013.

Infine, l'offerta su larga scala di nuovi servizi di refertazione con l'uso di nuove tecnologie deve essere preceduta da una valutazione d'impatto (DPIA) ai sensi dell'art. 35 GDPR e deve essere predisposta un'apposita procedura per la gestione dei *data breach*, che consenta di intervenire tempestivamente in caso di violazione del sistema di refertazione online e di monitorarne costantemente la sicurezza.

CHIARA RAUCCIO

<https://www.garanteprivacy.it/faq/referti-online>

2020/4(6)DPDM

### **La nuova indagine della Commissione europea per abuso di posizione dominante di Amazon**

Il 10 novembre 2020 la Commissione europea ha formalizzato l'avvio di una nuova procedura antitrust a carico della piattaforma e-commerce statunitense Amazon ai sensi degli articoli 11(6) del Regolamento del Consiglio No 1/2003 e 2(1) del Regolamento della Commissione No 773/2004.

Tale procedura si basa su un'ipotesi di abuso di posizione dominante da parte di Amazon tramite condotte distorsive della concorrenza al fine di favorire le proprie attività di vendita al dettaglio e/o dei venditori terzi che si servono dei servizi di logistica prestati dalla medesima Amazon, ossia di gestione dell'inventario, del magazzino, delle spedizioni e del servizio clienti (c.d. *Fulfillment by Amazon*). Questa indagine comprende tutta l'Area Economica Europea, ad eccezione del mercato italiano.

Il medesimo giorno la Commissione Europea recapitava ad Amazon, informando i regolatori degli Stati Membri dell'UE, una comunicazione di addebito relativa alla procedura avviata in data 17 luglio 2019, avente ad oggetto l'utilizzo fatto dalla società dei dati dei venditori operanti sulla propria piattaforma digitale ("*marketplace*"). Sebbene la Francia e la Germania siano indicati come i mercati più interessati per via del volume delle transazioni, anche tale procedura si estende a tutta l'Area Economica Europea. In questo caso l'addebito configura condotte ed effetti economici vietati dagli articoli 101 e 102 del TFUE.

In maggior dettaglio, le contestazioni della Commissione europea riguardano il duplice ruolo svolto dalla piattaforma Amazon sia di canale distributivo per aziende indipendenti, che di venditore di prodotti propri tramite il medesimo canale.

Infatti, si legge nella comunicazione di addebito che Amazon farebbe uso di informazioni non pubbliche raccolte attraverso il proprio *marketplace*, sulle vendite ed i prodotti di terzi venditori (quali il numero di ordini e di spedizioni per specifici prodotti, i ricavi del venditore, il numero di click alle offerte postate, i reclami e le restituzioni, altre misure di performance) per calibrare le offerte di vendita di prodotti propri e prendere decisioni strategiche a scapito delle aziende concorrenti. Una volta che tali informazioni confluiscono direttamente nel suo sistema automatizzato di aggregazione dei dati, Amazon ha la possibilità di sfruttarle per influenzare la visibilità dei suoi prodotti o di quelli di coloro che si avvalgono della logistica

Amazon tramite il canale “Buy Box”, con l’effetto di distorcere la concorrenza, abusando del proprio posizionamento di leader europeo tra i fornitori di servizi di mercato e-commerce.

Questa ipotesi accomuna la seconda investigazione ancora in fase preliminare, riguardante le condizioni ed i criteri che governano gli algoritmi di assegnazione ai venditori della permanenza nel “Buy Box”, oltre che i criteri di selezione dei venditori abilitati ad offrire i propri prodotti agli utenti del programma fedeltà “Prime”. Il fatto che nella sezione “Buy Box” dell’interfaccia della piattaforma digitale, ovvero lo spazio online attraverso il quale avvengono la maggior parte delle vendite su Amazon, sia mostrata l’offerta di un singolo venditore per prodotto scelto dal consumatore, direttamente acquistabile con un unico click, costituisce un vantaggio cruciale, così come l’accesso privilegiato ai clienti “Prime”, statisticamente maggiormente attivi e in costante crescita. Ne consegue che costituirebbe una distorsione della concorrenza favorire artificialmente la vendita dei prodotti Amazon o quelli dei venditori che utilizzano i suoi servizi di logistica attraverso tali canali.

In questa fase i due procedimenti avviati dalla Commissione europea non comprovano definitivamente l’esistenza di un’infrazione da parte di Amazon e non pregiudicano, dunque, la possibilità che vi sia un esito contrario alle allegazioni rese pubbliche dall’Autorità europea. Ad ogni modo, la Commissione darà priorità alla prosecuzione di tale indagine e spetterà ad Amazon iniziare a presentare le proprie difese, alla luce del fatto che, qualora fossero accertate le violazioni, la società rischia sanzioni nell’ordine dei miliardi di euro, ossia fino al 10% dei ricavi annuali in Europa. In alternativa, la società potrebbe decidere di adottare un approccio collaborativo con la Commissione al fine di trovare un accordo sulle sanzioni e i rimedi successivi che saranno imposti alla società.

DOMENICO PIERS DE MARTINO

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_2077](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077)

2020/4(7)LC

***Droits voisins e snippets: la Corte d’appello di Parigi conferma la decisione dell’Autorità garante della concorrenza francese nei confronti di Google.***

La Corte d’appello di Parigi, con l’*arrêt* dell’8 ottobre 2020, ha respinto il ricorso presentato da Google avverso la decisione n. 20-MC-01 della *Autorité de la Concurrence* del 9 aprile 2020 (l’“Autorità”), con la quale, constatato un pregiudizio grave ed immediato al settore della stampa per abuso di posizione dominante, l’Autorità ha ingiunto alla piattaforma di Mountain View di avviare e concludere entro tre mesi le negoziazioni con agenzie di stampa, organismi di gestione collettiva ed i maggiori editori francesi (ovvero i cd. titolari dei diritti sui contenuti) al fine di raggiungere un accordo sull’equa remunerazione per l’utilizzo dei contenuti di questi ultimi attraverso i cd. *snippets*. Trattasi di anteprime o estratti di notizie (letteralmente *fragmenti*), rinvenibili online gratuitamente sulle pagine dei collettori di news (nel caso di specie, Google News) che, di tal guisa, veicolano e utilizzano contenuti protetti dai diritti connessi al diritto d’autore (cd. *droits voisins*).

Segnatamente, l’Autorità ha accolto il ricorso presentato dall’AFP (*Alliance de la presse d’information générale*) e dagli organi di rappresentanza degli editori di giornali (*Syndicat des éditeurs de la presse magazine*), che chiedevano un’equa retribuzione per l’utilizzo dei loro contenuti, stabilendo, *inter alia*, che «(i)lest enjoint aux sociétés Google LLC, Google Ireland Ltd et Google France, à titre conservatoire et dans l’attente d’une décision au fond, de négocier de bonne foi avec les

*éditeurs et agences de presse ou les organismes de gestion collective qui en feraient la demande, la rémunération due par Google à ces derniers pour toute reprise des contenus protégés sur ses services, conformément aux modalités prévues à l'article L. 218-4 du code de la propriété intellectuelle et selon des critères transparents, objectifs et non discriminatoires»; ed aggiunge che «(c)ette négociation devra couvrir la période de reprise des contenus depuis le 24 octobre 2019», sancendone l'efficacia retroattiva.*

La vicenda s'inscrive nel più ampio quadro normativo recentemente riformato a livello europeo dalla direttiva 790/2019/UE del Parlamento europeo e del Consiglio del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale. Quest'intervento di armonizzazione della disciplina sul *copyright* si pone all'esito di un acceso dibattito, sia fuori che dentro le sedi istituzionali, che non può ancora dirsi del tutto sopito. In particolare, un *punctum dolens* della direttiva è ravvisabile, secondo le più note piattaforme digitali, nell'art. 15 che disciplina la "protezione delle pubblicazioni di carattere giornalistico in caso di utilizzo online", invocato nel caso di specie.

Cionondimeno, con quest'intervento, il legislatore europeo ha inteso armonizzare la disciplina *in subjecta materia* all'interno dei singoli Stati membri. Tra questi, la Francia è stato il primo Paese a recepire il 24 luglio 2019 la direttiva *copyright*, con la quasi unanimità dei voti in Parlamento (solo un voto contrario).

Il termine per il recepimento per gli altri Stati membri è fissato per il 7 giugno 2021, sebbene si registri un forte pressing da parte di autori ed editori – anche in Italia – affinché venga recepita in tempi brevi.

Con questa fondamentale decisione, inoltre, la Francia si candida come apripista anche sul terreno giurisprudenziale, offrendo un 'formante' con effetti che certamente travalicheranno i confini nazionali, riversandosi in tutti gli altri ordinamenti ed aprendo, *de facto*, un varco per l'avvio di negoziati nel settore di riferimento. In altri termini, la decisione appare destinata a riscrivere i rapporti tra le piattaforme digitali e i titolari dei diritti d'autore nel mercato unico digitale europeo.

LUCIO CASALINI

[https://www.autoritedelaconurrence.fr/sites/default/files/appealsd/2020-10/ca\\_20mc01\\_oct20.pdf](https://www.autoritedelaconurrence.fr/sites/default/files/appealsd/2020-10/ca_20mc01_oct20.pdf)

[https://www.autoritedelaconurrence.fr/sites/default/files/integral\\_texts/2020-04/20mc01.pdf](https://www.autoritedelaconurrence.fr/sites/default/files/integral_texts/2020-04/20mc01.pdf)

2020/4(8)SO

### **La Sapienza aderisce alla "Rome Call for AI Ethics".**

Il 30 ottobre 2020 l'Università Sapienza di Roma ha formalizzato la sua adesione alla "Rome Call for AI Ethics", con la firma del documento da parte del Rettore Eugenio Gaudio, alla presenza di Mons. Vincenzo Paglia, Presidente della Pontificia Accademia per la Vita.

"Rome Call for AI Ethics", promossa dalla Pontificia Accademia per la Vita, è stata presentata il 28 febbraio 2020 e ha avuto come primi firmatari rappresentanti della FAO, del Governo italiano, di Microsoft ed IBM, come riportato nella notizia [2020/1\(7\)LC](#).

Il documento, inteso a promuovere un'opera di sensibilizzazione intorno ai temi dell'"etica" della intelligenza artificiale, in particolare con riferimento alle sue possibilità di perpetuare ed amplificare discriminazioni e pratiche lesive della libertà degli esseri umani e della dignità dei soggetti più vulnerabili, individua sette principi, da sviluppare in ambito

educativo e giuridico, per una c.d. “*algorethical vision*”: trasparenza, inclusione, responsabilità, imparzialità, affidabilità, sicurezza e privacy.

SALVATORE ORLANDO

<https://www.uniroma1.it/it/notizia/sapienza-ha-aderito-alla-rome-call-ai-ethics-un-approccio-etico-allintelligenza-artificiale#:~:text=per%20la%20Vita-Venerdi%2030%20ottobre%202020%20è%20stata%20formalizzata%20l'adesione%20della,Gaudio%2C%20alla%20presenza%20di%20Mons.&text=Fare%20scelte%20etiche%20oggi%20significa%20cercare%20di%20trasformare%20il%20progresso%20in%20sviluppo>



## ANNO 2021

<a href="#">2021/1(1)DPDM</a>	
La “rivoluzione digitale” e lo European Democracy Action Plan del 03.12.2020 .....	p. 57
<a href="#">2021/1(2)GC</a>	
La strategia digitale della Risoluzione del Parlamento Europeo del 25.11.2020 “Verso un mercato unico più sostenibile per le imprese e i consumatori” .....	p. 58
<a href="#">2021/1(3)ST</a>	
Verso il Digital Services Act: la Proposta di Regolamento sul “mercato unico dei servizi digitali” del 15.12.2020 .....	p. 59
<a href="#">2021/1(4)EMI</a>	
Verso il Digital Markets Act: la Proposta di Regolamento su “mercati equi e contendibili nel settore digitale” del 15.12.2020 .....	p. 65
<a href="#">2021/1(5)RMo</a>	
Il parere del 10.02.2021 dello EDPS sulla proposta del Digital Services Act in particolare sulla pubblicità mirata e i recommender systems .....	p. 65
<a href="#">2021/1(6)LC</a>	
La Risoluzione del 21.01.2021 del Parlamento europeo sul diritto dei lavoratori alla disconnessione .....	p. 67
<a href="#">2021/1(7)FR</a>	
Regolamento P2B e nuove funzioni delle Autorità indipendenti alla luce della Legge di Bilancio 2021 .....	p. 68
<a href="#">2021/1(8)CR</a>	
Clearview AI condannata in Germania per violazione del GDPR: il caso Marx	p. 69
<a href="#">2021/1(9)CM</a>	
Apple condannata dal Tribunale di Milano a fornire accesso al patrimonio digitale di un defunto (ordinanza del 09.02.2021) .....	p. 70
<a href="#">2021/2(1)SO</a>	
Verso l’Artificial Intelligence Act: la Proposta di Regolamento del 21.04.2021 su regole armonizzate in materia di intelligenza artificiale .....	p. 72
<a href="#">2021/2(2)CR</a>	
Il comunicato del 23.04.2021 dello EDPS sulla proposta dell’ <i>Artificial Intelligence Act</i> in particolare sul riconoscimento facciale .....	p. 79
<a href="#">2021/2(3)CR</a>	
Il parere del Garante Privacy del 16.04.2021 sul sistema di riconoscimento facciale SARI Real Time da parte del Ministero dell’Interno .....	p. 80
<a href="#">2021/2(4)FP</a>	
Lo studio del 05.02.2021 pubblicato dal Parlamento europeo sulla responsabilità delle piattaforme online .....	p. 81
<a href="#">2021/2(5)FP</a>	
I Final Reports del marzo 2021 del gruppo di esperti dell’Osservatorio sulla platform economy .....	p. 83
<a href="#">2021/2(6)EP</a>	
Il Parere della BCE del 19.02.2021 sulla Proposta di Regolamento sui mercati di crypto-assets .....	p. 85

<a href="#">2021/2(7)EP</a>	Il comunicato di Consob e Banca d'Italia sui crypto-assets del 28.04.2021 .....	p. 87
<a href="#">2021/2(8)MG</a>	La sentenza 2631 del Consiglio di Stato del 29.03.2021 nel caso Facebook (gratuità del servizio e divieto di pratiche commerciali scorrette) .....	p. 88
<a href="#">2021/2(9)DPDM</a>	La comunicazione di addebiti del 30.04.2021 della Commissione europea ad Apple per abuso di posizione dominante per le regole delle app di musica in streaming su App Store .....	p. 89
<a href="#">2021/2(10)EMI</a>	Fair use e open source: la decisione della Corte Suprema degli Stati Uniti d'America del 05.04.2021 nel caso delle API di Java (Oracle c/ Google) .....	p. 90
<a href="#">2021/3(1)DI</a>	La Carta dei diritti digitali presentata dal Governo spagnolo il 14 luglio 2021..	p. 92
<a href="#">2021/3(2)SO-CS</a>	La Corte di Cassazione subordina la validità del consenso al trattamento dei dati personali alla trasparenza dell'algoritmo che governa il servizio per il quale il consenso è prestato (ordinanza 14381 del 25 maggio 2021 a proposito di un servizio di calcolo del c.d. <i>rating</i> reputazionale) .....	p. 93
<a href="#">2021/3(3)CR</a>	Il pronunciamento congiunto EDPS - EDPB del 21 giugno 2021 sulla proposta di disciplina sul riconoscimento facciale contenuta nell' <i>Artificial Intelligence Act</i> .....	p. 95
<a href="#">2021/3(4)CM</a>	Le regole sul riconoscimento facciale per le società private emesse dalla Suprema Corte del Popolo della Repubblica Popolare Cinese il 28 luglio 2021	p. 97
<a href="#">2021/3(5)LV</a>	Le Linee Guida EDPB del 7 luglio 2021 sugli assistenti vocali virtuali .....	p. 98
<a href="#">2021/3(6)CR</a>	Le Linee Guida del Garante Privacy italiano sui cookies ed altri strumenti di tracciamento del 10 giugno 2021 .....	p. 100
<a href="#">2021/3(7)AF</a>	La decisione del Consiglio direttivo della BCE del 12 luglio 2021 di avviare l'analisi del progetto per un "euro digitale" .....	p. 102
<a href="#">2021/3(8)FP</a>	La Repubblica di El Salvador adotta il Bitcoin come moneta avente corso legale nel Paese (la " <i>Ley Bitcoin</i> " dell'8 giugno 2021) .....	p. 103
<a href="#">2021/3(9)AN</a>	Il provvedimento del 22 luglio 2021 del Garante Privacy nei confronti di Deliveroo per il trattamento dei dati personali dei riders .....	p. 106
<a href="#">2021/3(10)CM</a>	Il pronunciamento del 28 maggio 2021 della Suprema Corte del Popolo della Repubblica Popolare Cinese sul valore probatorio dei dati registrati su blockchain .....	p. 108
<a href="#">2021/4(1)FB</a>	Il recepimento in Italia delle direttive (UE) 2019/770 e 2019/771 relative a determinati aspetti dei contratti di fornitura di contenuti e servizi digitali e a determinati aspetti dei contratti di vendita di beni di consumo .....	p. 108

<a href="#">2021/4(2)FP</a>	
Il recepimento in Germania della direttiva (UE) 2019/770 .....	p. 114
<a href="#">2021/4(3)CR</a>	
Le rilevanti modifiche al Codice Privacy introdotte dal ‘Decreto Capienze’ del 7 ottobre 2021 come convertito in legge con modifiche ad opera della legge 3 dicembre 2021 n. 205 .....	p. 117
<a href="#">2021/4(4)RA</a>	
Verso il Data Governance Act: le modifiche del Consiglio dell’Unione Europea del 24 settembre 2021 alla proposta di regolamento della Commissione, approvate dal Comitato dei rappresentanti permanenti il 1 ottobre 2021 con contestuale mandato alla Presidenza del Consiglio di avviare le negoziazioni con il Parlamento Europeo .....	p. 119
<a href="#">2021/4(5)EMI</a>	
La sentenza della Corte di Giustizia UE del 6 ottobre 2021 sul diritto di decompilazione del software (il caso <i>Top System</i> ) .....	p. 123
<a href="#">2021/4(6)FG</a>	
La sentenza della Court of Appeal del 21 settembre sul caso Dabus: l’intelligenza artificiale può essere considerata inventore? .....	p. 125
<a href="#">2021/4(7)FDA</a>	
La sentenza del Tar Lazio n. 7589 del 24 giugno 2021 su algoritmi e attività amministrativa (a proposito di procedure di mobilità nella Pubblica Amministrazione) .....	p. 128
<a href="#">2021/4(8)VR</a>	
L’ordinanza del 16 settembre 2021 del Garante Privacy a proposito del sistema software di supervisione degli studenti “Respondus” impiegato dall’Università Bocconi di Milano per le prove scritte di esame .....	p. 129
<a href="#">2021/4(9)ES</a>	
L’apertura della prima finestra temporale sulla sandbox regolamentare per i progetti fintech di cui al Decreto del MEF n. 100 del 30 aprile 2021 .....	p. 133
<a href="#">2021/4(10)AF</a>	
Il rapporto del 13 ottobre 2021 dei Ministeri dell’Economia e delle Banche Centrali dei Paesi G7 " <i>Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)</i> " .....	p. 135
<a href="#">2021/4(11)SS</a>	
Le Classi di rischio dei ‘Software As Medical Devices’ (SAMDs) alla data di piena applicazione del Regolamento 2017/745 UE sui dispositivi medicali .....	p. 137
<a href="#">2021/4(12)BC</a>	
La legge dello Stato del <i>Wyoming</i> sulle <i>Decentralized Assets Organizations</i> (DAOs) del 21 aprile 2021 .....	p. 138
<a href="#">2021/4(13)CM</a>	
La prima legge sulla protezione delle informazioni personali della Repubblica Popolare Cinese (la ‘PIPL’) .....	p. 141



2021/1(1)DPDM

**La “rivoluzione digitale” e lo *European Democracy Action Plan* del 03.12.2020.**

Con la comunicazione COM790 (2020) final del 3 dicembre 2020 (la “**Comunicazione**”), la Commissione europea ha presentato il suo “Piano d'azione per la democrazia europea” finalizzato alla fortificazione della democrazia in tutta l'Unione Europea, a fronte di quella che nella Comunicazione viene definita come la “trasformazione digitale delle nostre democrazie” e anche la “rivoluzione digitale”. Questo piano costituisce una delle principali iniziative dell'agenda politica del Presidente della Commissione von der Leyen.

Il tema centrale della Comunicazione è quello dei pericoli in cui incorrono le democrazie europee a causa degli abusi del potere mediatico, con la rivoluzione digitale in corso. In particolare, il piano ha il fine di promuovere ulteriormente una società in cui le persone siano messe nelle condizioni di compiere scelte libere ed esprimere le proprie opinioni in un contesto in cui, allo stesso tempo, i canali di comunicazione non diventino strumenti di manipolazione facenti capo a pochi centri di interesse.

Più in dettaglio, nella Comunicazione viene detto che la crescita delle campagne elettorali *online* e le modalità di utilizzo delle piattaforme di comunicazione hanno reso più difficile preservare l'integrità delle elezioni, garantire media liberi e plurali, e proteggere il processo democratico dalla disinformazione e da altre interferenze. Si osserva che la digitalizzazione consente la diffusione di nuovi e non monitorabili metodi di finanziamento ai partiti, i *cyber*-attacchi possono prendere di mira le “infrastrutture elettorali” e le false informazioni possono essere diffuse rapidamente sui social media, anche attraverso campagne di disinformazione coordinate. Si aggiunge che l'impatto di alcuni di questi fenomeni è amplificato dall'uso di algoritmi non trasparenti i quali sono controllati da piattaforme aventi *network* diffusi a livello globale.

In risposta a ciò, il piano d'azione per la democrazia europea individua tre aree di intervento. Esso stabilisce misure per promuovere elezioni libere ed eque, rafforzare il pluralismo dei media e contrastare la disinformazione. Per quanto riguarda il rafforzamento dell'integrità delle elezioni politiche, la Commissione propone di introdurre una legislazione sulla trasparenza dei contenuti politici sponsorizzati e intende rivedere le regole sul finanziamento dei partiti politici europei, mirando a rafforzare la cooperazione tra gli Stati membri. Per difendere il pluralismo mediatico, invece, la Commissione innanzitutto riconosce la necessità di supportare l'intera classe dei giornalisti contro minacce o cause legali pretestuose intentate col mero fine di dissuadere quest'ultimi dal prender parte all'offerta di informazione nell'interesse della collettività. Nella medesima direzione vanno le linee di proposta volte a rafforzare la trasparenza relativa agli assetti proprietari dei media, attraverso un nuovo osservatorio *ad hoc*, e alla pubblicità statale.

Infine, il piano della Commissione comprende la necessità di rivedere il *Code of Practice on Disinformation*, vale a dire il codice di condotta, contenente gli standard regolamentari per combattere la disinformazione, a cui le piattaforme *online*, i principali *social network*, gli inserzionisti e l'industria pubblicitaria possono vincolarsi su base volontaria. La revisione fornirà un quadro di obblighi e responsabilità a carico delle piattaforme digitali, in linea con il *Digital Services Act* (su cui v. *infra* in questa Rubrica sub **3**). Questi sforzi sono diretti anche a contrastare le crescenti interferenze straniere all'interno dei singoli Stati Membri, rese possibili con l'avvento della rivoluzione digitale, attraverso la costituzione di strumenti per imporre sanzioni ai perpetratori di eventuali attacchi alla democrazia europea.

DOMENICO PIERS DE MARTINO

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423>

2021/1(2)GC

**La strategia digitale della Risoluzione del Parlamento Europeo del 25.11.2020 “*Verso un mercato unico più sostenibile per le imprese e i consumatori*”**

La Risoluzione del Parlamento Europeo del 25 novembre 2020 sul tema “*Verso un mercato unico più sostenibile per le imprese e i consumatori*” (2020/2021 INI) (la “**Risoluzione**”) si inserisce in un quadro di evoluzione della normativa dell’Unione Europea, volto a costruire una rinnovata opzione macroeconomica di sistema che faccia propria la dimensione della sostenibilità, attraverso un insieme di regole e di riconoscimenti di diritti e tutele fondamentali. La Risoluzione dedica un capo alla strategia digitale confermandone il carattere di infrastruttura del mercato sostenibile.

Nei considerando R e S della Risoluzione si parla delle piattaforme *online* e del tema strategico dell’informazione. L’accesso alle piattaforme e la diffusione delle informazioni possono rappresentare la garanzia non solo per i consumatori, ma anche per costruire un diverso tipo di democrazia, se non diretta, certamente maggiormente partecipata. E le garanzie di cui devono essere dotate le informazioni e i processi connessi alle piattaforme *online* devono tener conto di queste implicazioni. Il considerando T ribadisce la necessità di valutare l’impatto ambientale dell’infrastruttura digitale.

Nel capo della Risoluzione dedicato alla strategia digitale al servizio di un mercato sostenibile, al par. 21, si segnala che l’Unione Europea accoglie con favore l’annuncio di uno spazio comune europeo dei dati per le *applicazioni circolari intelligenti* e vuole sviluppare appunto un *passaporto dei prodotti digitale* per migliorare tracciabilità e accesso alle informazioni sulle condizioni di produzione di un prodotto, la durabilità, la composizione di un prodotto, il riutilizzo, la riparazione e tutta una serie di aspetti che possono riguardare la riparabilità e anche lo smaltimento, eventualmente, del prodotto. In questo quadro, lo spazio europeo dei dati per le applicazioni circolari intelligenti fornirà l’architettura e il sistema di *governance* per stimolare applicazioni e servizi, quali i passaporti dei prodotti, la mappatura delle risorse e l’informazione ai consumatori. Di fatto il par. 21 risponde all’esigenza di creare un sistema di dati che consenta di tracciare e accedere alle informazioni relative alla produzione di un certo prodotto, il che può essere costruito attraverso la tecnologia *Blockchain*. Strettamente correlato a questo tema c’è quello della certificazione, cui il passaporto offre una base documentata.

L’economia circolare, al par. 22, rappresenta una delle linee della trasformazione industriale verso temi centrali della sostenibilità, quali la neutralità climatica e la competitività a lungo termine, sfruttando le tecnologie digitali per quanto riguarda la tracciabilità, la rintracciabilità e la mappatura delle risorse e delle tecnologie verdi. A fronte del significativo impatto ambientale del settore digitale, il par. 23, per quanto concerne la produzione di beni e la fornitura di servizi, invita la Commissione a valutare in che misura un indice di sostenibilità del digitale europeo che sia basato su un’analisi del ciclo di vita dei prodotti possa ottimizzare la produzione e il consumo sostenibili di tecnologie digitali, in quanto è estremamente importante scegliere un adeguato criterio di valutazione. Il par. 24 riguarda la potenziale impronta ambientale dei dati che non siano necessari e cioè applicazioni, o file, video, foto, messaggi di posta elettronica che siano indesiderati e che quindi, avendo una

qualunque impronta ambientale causino un eccessivo dispendio energetico. Il par. 25 contempla i sistemi di ricarica universale per ridurre la produzione e ridurre anche i rifiuti e i rifiuti elettronici.

Un ulteriore elemento degno di nota riguarda la digitalizzazione degli appalti, al paragrafo 26.

GIUSEPPINA CAPALDO

[https://www.europarl.europa.eu/doceo/document/A-9-2020-0209\\_IT.pdf](https://www.europarl.europa.eu/doceo/document/A-9-2020-0209_IT.pdf)

2021/1(3)ST

### **Verso il *Digital Services Act*: la Proposta di Regolamento sul “mercato unico dei servizi digitali” del 15.12.2020**

La significativa evoluzione del settore digitale si accompagna al delinearci di un modello di *business* nel quale alcuni operatori assumono un ruolo strategico. Sono in grado, infatti, di indirizzare le scelte dei consumatori e controllare l'accesso e la permanenza sul mercato delle imprese. Partendo da tale consapevolezza, è sempre più avvertita l'esigenza di una regolamentazione, fino ad ora prevalentemente affidata alla direttiva 2000/31/CE sul commercio elettronico e al regolamento (UE) 2019/1150, che promuova equità e trasparenza per gli utenti dei servizi di intermediazione *online*.

In questo scenario si colloca la recente proposta del cd. *Digital Services Act* ossia la *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE*, COM(2020) 825 final del 15 dicembre 2020.

Si tratta di un provvedimento molto complesso che mira a stabilire regole uniformi per un ambiente *online* sicuro, prevedibile e affidabile, soprattutto dopo le singole iniziative legislative intraprese da alcuni Stati membri, quali, per esempio, il tedesco *Netzwerkdurchsetzungsgesetz* (c.d. *NetzDG*) del 2017 e la francese *Loi contre les contenus haineux sur internet* (c.d. *Loi Avia*) del 2020 (su cui v. [2020/2\(6\)DI](#)).

Nelle intenzioni della relativa proposta, il *Digital Services Act* (“**DSA**”) è complementare al c.d. *Digital Markets Act* (su cui v. *infra* in questo numero di questa Rubrica sub 4.), che si occupa, in modo più specifico, dei comportamenti delle aziende che hanno assunto una rilevanza sistemica come c.d. *gatekeeper*.

Entrambi i provvedimenti si inseriscono nel percorso segnato dallo *Shaping Europe's Digital Future*, con il quale la Commissione europea si è impegnata ad aggiornare le norme che definiscono le responsabilità e gli obblighi dei fornitori di servizi digitali, e in particolare delle piattaforme *online*.

La proposta di Regolamento sul DSA prevede: “a) un quadro per l'esenzione condizionata dalla responsabilità dei prestatori di servizi intermediari; b) norme relative a specifici obblighi in materia di dovere di diligenza adattati a determinate categorie di prestatori di servizi intermediari; c) norme sull'attuazione e sull'esecuzione del presente regolamento, anche per quanto riguarda la cooperazione e il coordinamento tra le autorità competenti.” (art. 1, para. 1).

Il DSA si pone in continuità con le scelte di base della direttiva sul commercio elettronico e, in particolare, con quelle relative al principio del mercato interno di cui all'articolo 3 e

all'assenza di un obbligo generale di sorveglianza a carico dei prestatori di servizi di intermediazione *ex art. 15*.

È proposta la soppressione, è vero, degli articoli dal 12 al 15 della direttiva sul commercio elettronico, ma, conformemente all'interpretazione della Corte di giustizia dell'Unione, vengono previste disposizioni sulle condizioni in base alle quali i fornitori di servizi di *conduit*, *caching* e di *hosting* sono esentati dalla responsabilità per le informazioni di terzi che trasmettono e memorizzano.

Filo conduttore della nuova regolamentazione, proposta con il DSA, è l'adeguamento degli obblighi di diligenza al tipo e alla natura del servizio di intermediazione interessato. A tal fine, si prevedono obblighi di base applicabili a tutti i fornitori di servizi di intermediazione, ma anche obblighi aggiuntivi per le piattaforme *online*, con specifiche disposizioni per le piattaforme *online* di dimensioni molto grandi (*very large online platforms*). Si delinea una logica proporzionale e cumulativa nell'imposizione di obblighi, che aumentano e si sommano a mano a mano che i fornitori di servizi di intermediazione siano qualificabili come *hosting*, piattaforme *online* o *very large online platforms*.

La sottocategoria delle piattaforme *online* è costituita dai fornitori di servizi di *hosting* che, non solo memorizzano le informazioni fornite dai destinatari del servizio su loro richiesta, ma diffondono anche tali informazioni al pubblico.

Le *very large online platforms* sono quelle che prestano i loro servizi a un numero medio mensile di destinatari attivi nell'Unione pari o superiore a 45 milioni (art. 25).

Il primo livello di obblighi riguarda quelli applicabili a tutti i fornitori di servizi di intermediazione. Si tratta di obblighi di trasparenza e obblighi di coordinamento. Questi ultimi sono volti a favorire comunicazioni dirette ed efficaci con le Autorità degli Stati membri, la Commissione e il "Comitato europeo per i servizi digitali" (in inglese lo *European Board for Digital Services*), di cui è prevista l'istituzione a mezzo dello stesso DSA *ex art. 47* (il "**Comitato**"). In particolare, i fornitori di servizi di intermediazione devono istituire un "punto di contatto unico" che consenta la comunicazione diretta, per via elettronica, con le autorità degli Stati membri, la Commissione e il Comitato, e rendere pubbliche le informazioni necessarie per identificarlo (art. 10).

I *provider* che non hanno stabilimenti nell'Unione, ma che offrono i propri servizi all'interno della stessa, dovranno, *ex art. 11*, designare un legale rappresentante, dotato di poteri e risorse necessarie per cooperare con le Autorità degli Stati membri, la Commissione e il Comitato. Tale rappresentante sarà responsabile, ai sensi del co. 3 dell'art. 11, in caso di mancato rispetto degli obblighi previsti dal DSA.

Una significativa novità è apportata dagli obblighi di trasparenza imposti a tutti gli intermediari e riguardanti eventuali limitazioni all'uso dei servizi offerti. Tali limitazioni, infatti, devono essere incluse nei termini e nelle condizioni contrattuali. Queste ultime devono, altresì, contenere informazioni su eventuali procedure, misure e strumenti di moderazione dei contenuti (*content moderation*), specificando se questi siano sottoposti ad *algorithmic decision-making* o a *human review*. Alla *content moderation* è dedicata particolare attenzione sia in quanto si impone annualmente, *ex art. 13*, di produrre relazioni chiare, facilmente comprensibili e dettagliate sulle attività di moderazione dei contenuti, sia in quanto si specifica che i fornitori di servizi di intermediazione devono agire in modo diligente, obiettivo e proporzionato nell'applicare e far rispettare le eventuali restrizioni all'uso del loro servizio.

Gli obblighi aumentano poi, proporzionalmente, con le disposizioni aggiuntive riguardanti i prestatori di servizi di *hosting*, comprese le piattaforme *online*. L'obiettivo è armonizzare la normativa relativa alla lotta e alla gestione dei contenuti illegali *online* ed evitare che vengano erroneamente rimossi contenuti legali. A tal fine è previsto che i prestatori di

servizi di *hosting* debbano predisporre meccanismi di facile accesso e uso per consentire a qualsiasi persona o ente di notificare la presenza di contenuti illegali.

La comunicazione di un contenuto illecito deve avvenire in modo sufficientemente preciso e con adeguata motivazione. L'art. 14 prevede, infatti, un minuzioso "Meccanismo di notifica e azione" (*Notice and action mechanisms*) che mira a superare i tanti dubbi interpretativi posti dall'art. 14 della direttiva sul commercio elettronico e affrontati in numerosi casi dalla Corte di Giustizia. Obblighi specifici di motivazione (*statement of reasons*), sono previsti dall'art. 15 per il prestatore di servizi di *hosting* che decida di rimuovere specifiche informazioni fornite dai destinatari del servizio o disabilitare l'accesso alle stesse. In particolare, il fornitore del servizio deve informare il destinatario della sua decisione, delle ragioni della stessa (ragioni che devono consistere nell'indicazione di alcune informazioni minime, elencate nel medesimo art. 15) e dei mezzi disponibili per impugnarla. Emerge la consapevolezza delle possibili conseguenze negative che tali decisioni possano avere per il destinatario, anche per quanto riguarda l'esercizio del suo diritto fondamentale alla libertà di espressione.

Da questo punto di vista, il DSA mira a rappresentare, insieme allo *European Democracy Action Plan* (su cui v. *supra* in questo numero di questa Rubrica sub 1.), un elemento di svolta nella lotta all'*hate speech* digitale, puntando su obblighi di trasparenza da parte dei *provider* e sulla predisposizione di opportune garanzie procedurali a favore degli utenti.

Nelle sezioni del DSA che seguono si entra nello specifico del differente apparato di obblighi a seconda delle dimensioni delle piattaforme e dell'influenza che possono avere sulle scelte, di mercato e di vita, degli *user*.

Un ulteriore gruppo di disposizioni aggiuntive riguarda le piattaforme *online*, ad esclusione di quelle che sono *micro* o piccole imprese ai sensi dell'Allegato alla Raccomandazione 2003/361/CE. Si tratta di dettagliati obblighi relativi al sistema interno di gestione dei reclami (art. 17), che deve avvenire in modo tempestivo, diligente e obiettivo, assicurando una continua interazione con i reclamanti.

Il sistema previsto mira ad evitare che si abusì della possibilità delle notifiche, nell'ottica di un equilibrio tra i diversi interessi coinvolti. A tal fine, l'attendibilità delle segnalazioni è calibrata sulla provenienza delle stesse, ma anche su eventuali precedenti segnalazioni risultate manifestamente infondate. In tale logica si giustifica che le piattaforme *online* debbano garantire che le notifiche presentate dai c.d. *trusted flaggers*, ossia dai segnalatori attendibili, identificati come tali dal competente "Coordinatore dei servizi digitali" (organo previsto dai considerando n. 73 e ss. e dall'art. 38), siano trattate con priorità.

Al fine di contrastare la vendita di prodotti contraffatti *online* è prevista la cd. Tracciabilità degli operatori commerciali (art. 22). Le piattaforme *online* - qualora consentano agli operatori commerciali di utilizzare i propri servizi per pubblicizzare o offrire prodotti ai consumatori - devono ottenere le informazioni necessarie per l'identificazione del professionista secondo il modello del cd. "*Know your customer*" (KYC). Rispetto a tali informazioni, il ruolo delle piattaforme *online* non può essere meramente passivo, in quanto sono tenute a compiere sforzi ragionevoli, ai sensi dell'art. 22, per stabilire se le stesse siano attendibili.

È, altresì, obbligatorio redigere un *transparency reporting* con informazioni aggiuntive rispetto a quelle previsti dall'art. 13 per tutti gli intermediari.

La trasparenza riguarda anche la pubblicità *online* e, pure in questo caso, si applica una logica di imposizione di obblighi crescenti, in proporzione alle dimensioni della piattaforma.

L'*online advertising transparency* è affidata, in prima battuta, ad alcuni obblighi che riguardano tutte le piattaforme e che sono delineati dall'art. 24. Ogni singolo destinatario del messaggio pubblicitario, infatti, deve essere in grado di identificare, in modo chiaro e non ambiguo, e in tempo reale, la natura pubblicitaria delle informazioni visualizzate, la persona fisica o

giuridica per conto della quale viene visualizzata la pubblicità, nonché le informazioni rilevanti sui principali parametri utilizzati per determinare il destinatario al quale viene mostrata la pubblicità.

Obblighi supplementari di trasparenza riguardano le piattaforme *online* di dimensioni molto grandi, che, infatti, sono tenute a compilare e rendere disponibile al pubblico, attraverso le interfacce di programmazione delle applicazioni, un registro contenente, come minimo, le informazioni previste dall'art. 30 e poste anche a garanzia di pubblicità destinate ad uno o più gruppi specifici di soggetti.

Gli obblighi aggiuntivi per le piattaforme *online* di dimensioni molto grandi non si limitano a quelli evidenziati con riferimento alla pubblicità, ma ad essi è dedicata tutta la Sezione IV del Capo III del DSA che riguarda i rischi sistemici. In particolare, le piattaforme *online* di dimensioni molto grandi sono tenute, almeno una volta all'anno, ad individuare, analizzare e valutare, *ex art. 26*, eventuali rischi sistemici significativi derivanti dal funzionamento e dall'uso dei loro servizi nell'Unione, anche sulla base dei valori espressi dalla Carta dei diritti fondamentali dell'Unione europea (la “**Carta**”).

Ai sensi dell'art. 26, tali rischi sono riconducibili a tre categorie: “a) la diffusione di contenuti illegali tramite i loro servizi; b) eventuali effetti negativi per l'esercizio dei diritti fondamentali al rispetto della vita privata e familiare e alla libertà di espressione e di informazione, del diritto alla non discriminazione e dei diritti del minore, sanciti rispettivamente dagli articoli 7, 11, 21 e 24 della Carta; c) la manipolazione intenzionale del servizio, anche mediante un uso non autentico o uno sfruttamento automatizzato del servizio, con ripercussioni negative, effettive o prevedibili, sulla tutela della salute pubblica, dei minori, del dibattito civico, o con effetti reali o prevedibili sui processi elettorali e sulla sicurezza pubblica”.

L'attività di *risk assessment* è propedeutica all'adozione di misure di attenuazione ragionevoli, proporzionate ed efficaci, adattate agli specifici rischi sistemici individuati. I risultati della valutazione di tali rischi e delle relative misure di mitigazione formano oggetto di una relazione che le *very large online platforms* devono trasmettere al Coordinatore dei servizi digitali del luogo di stabilimento e alla Commissione, in adempimento alle obbligazioni di comunicazione trasparente di cui all'art. 33.

Le piattaforme *online* di dimensioni molto grandi, inoltre, hanno l'obbligo di sottoporsi, a proprie spese e almeno una volta all'anno, ad *audit*, esterni e indipendenti, volti a verificare la conformità della loro condotta agli obblighi previsti.

Ulteriori obblighi sono previsti dall'art. 29 con riferimento ai “sistemi di raccomandazione” (*recommender systems*, definiti nell'art. 2 lett. o), in particolare, l'obbligo di specificare nelle condizioni generali, in modo chiaro, accessibile e facilmente comprensibile, i principali parametri utilizzati, nonché qualunque opzione messa a disposizione dei destinatari del servizio per consentire loro di modificare o influenzare i parametri principali.

Le piattaforme *online* di dimensioni molto grandi hanno, nei confronti del Coordinatore dei servizi digitali del luogo di stabilimento o della Commissione, obblighi di *disclosure* dei dati necessari per monitorare e valutare la conformità della loro condotta al DSA.

Tra le figure preposte al controllo e al monitoraggio del rispetto del DSA, da parte dell'organizzazione delle piattaforme *online* di grandi dimensioni, i “responsabili di conformità” (*compliance officers*) (art. 32), che possono essere dipendenti delle piattaforme oppure svolgere le loro funzioni sulla base di un contratto con le stesse. In entrambi i casi, però, devono essere adottate le misure necessarie per far sì che i responsabili della conformità possano svolgere i loro compiti in modo indipendente.

La proposta di regolamento in oggetto si pone nel solco dell'orientamento dell'Unione Europea particolarmente fiducioso negli strumenti di autoregolazione. Lo si evince dagli

ulteriori obblighi di diligenza previsti dal DSA e relativi all'elaborazione ed allo sviluppo di codici di condotta specifici per la pubblicità *online*. Disposizioni alle quali si aggiungono quelle sui protocolli di crisi per affrontare circostanze straordinarie che incidono sulla sicurezza pubblica o sulla salute pubblica (art. 34-37).

Le novità in punto di *governance* chiudono il DSA che prevede una o più Autorità competenti designate a garantire l'applicazione del regolamento. Tra queste autorità competenti c'è quella, sopra già menzionata, dei 'Coordinatori dei servizi digitali' (*Digital Services Coordinators*) (considerando 73 ss., art. 38).

Ad arricchire ulteriormente l'apparato burocratico c'è il già menzionato Comitato (lo *European Board for Digital Services*), definito come "gruppo consultivo indipendente di Coordinatori dei servizi digitali per la vigilanza sui prestatori di servizi intermediari" (art. 47). Il Comitato fornisce consulenza ai Coordinatori dei servizi digitali e alla Commissione sull'applicazione del Regolamento, assistendoli anche nell'attività di vigilanza sulle piattaforme di grandi dimensioni. Oltre a poteri consultivi, di coordinamento e di assistenza, il Comitato ha il compito di promuovere l'elaborazione e l'attuazione di norme, orientamenti, relazioni, modelli e codici di condotta europei.

Parallelamente ad obblighi più stringenti, è prevista per le piattaforme *online* di dimensioni molto grandi una vigilanza rafforzata che si articola in un procedimento le cui fasi sono dettagliatamente disciplinate, anche al fine di garantire il contraddittorio e l'accesso agli atti. Su raccomandazione del Comitato o di propria iniziativa previa consultazione del Comitato, nel procedimento può intervenire la Commissione che può richiedere informazioni ed ha, altresì, poteri di audizione e di raccogliere dichiarazioni (art. 53) e di effettuare ispezioni *in loco* (art. 54).

Ancora, è previsto che qualora la Commissione accerti che la *very large online platform* non rispetti le disposizioni del Regolamento, o le misure provvisorie ordinate o gli impegni resi vincolanti, adotti la cd. decisione di non conformità (*non-compliance decision*) (art. 58), sia pure a seguito di contestazioni preliminari motivate e che contengono una spiegazione delle misure che la Commissione intende adottare, o che ritiene che la piattaforma *online* di dimensioni molto grandi dovrebbe adottare. Qualora la Commissione constati che le condizioni da essa richiesta non siano state soddisfatte, l'indagine potrà essere chiusa con una decisione che può prevedere sanzioni pecuniarie non superiori al 6% del fatturato totale realizzato dalla piattaforma nell'esercizio precedente (art. 59).

L'intento è quello di un apparato sanzionatorio effettivo, proporzionato e dissuasivo, che tenga conto della natura, della gravità, della reiterazione e della durata della violazione, secondo una politica ormai costante dell'Unione e affidata prevalentemente ad una sanzione pecuniaria in percentuale del fatturato.

Il percorso verso a *human-centric technological model*, che prescinda anche dai limiti europei e si basi su un approccio globale, è ancora in salita, ma il DSA sarà una tappa importante, quantomeno per l'attenzione ai rischi dei servizi digitali e alla vulnerabilità dei diritti fondamentali degli utenti, che non possono avere un ruolo di secondo piano rispetto alle potenzialità del commercio elettronico ed alla sua portata trainante per il rilancio dell'economia europea.

SARA TOMMASI

<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN>  
<https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0825&from=en>

2021/1(4)EMI

### **Verso il *Digital Markets Act*: la Proposta di Regolamento su “mercati equi e contendibili nel settore digitale” del 15.12.2020**

Il 15 dicembre 2020 la Commissione europea ha pubblicato la *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale* (c.d. *Digital Markets Act* o, nella versione italiana della proposta, “legge sui mercati digitali”), COM(2020) 842 final. La proposta si inserisce nella più ampia strategia digitale dell’Unione Europea (*Shaping Europe’s Digital Future*) ed insieme alla proposta sul c.d. *Digital Services Act* (su cui v. *supra* in questa Rubrica sub **3.**) mira a garantire uno spazio virtuale sicuro e a costituire un *level playing field* che favorisca l’innovazione e la competitività nel mercato europeo.

La proposta prevede che il *Digital Markets Act* (“**DMA**”) si applichi alle piattaforme digitali che hanno assunto una rilevanza sistemica all’interno del mercato unico digitale ed alle loro attività qualificate come “servizi di piattaforma di base”, definiti dall’art. 2, come uno qualunque dei seguenti servizi: “a) servizi di intermediazione *online*; b) motori di ricerca *online*; c) servizi di *social network online*; d) servizi di piattaforma per la condivisione di video; e) servizi di comunicazione interpersonale indipendenti dal numero; f) sistemi operativi; g) servizi di *cloud computing*; h) servizi pubblicitari, compresi reti pubblicitarie, scambi di inserzioni pubblicitarie e qualsiasi altro servizio di intermediazione pubblicitaria, erogati da un fornitore di uno dei servizi di piattaforma di base elencati alle lettere da a) a g)”.

La proposta si rivolge, in particolare, ai c.d. *gatekeeper* che offrono servizi di piattaforma di base, ovvero gli operatori che detengono il controllo dell’accesso in specifici settori e si connota per adottare un approccio regolatorio *ex ante*, diverso dal tradizionale controllo *ex post* della disciplina antitrust europea.

Ai sensi dell’art. 3, le piattaforme si qualificano come *gatekeeper* se: (i) hanno un impatto significativo sul mercato interno, (ii) gestiscono un servizio di piattaforma di base che costituisce un punto di accesso (*gateway*) tra gli utenti commerciali e gli utenti finali, e (iii) detengono una posizione consolidata e duratura nel proprio settore di mercato (o si prevede che la acquisiranno).

Il primo requisito si presume soddisfatto se l’impresa del fornitore dei servizi di piattaforma di base raggiunge un fatturato annuo nello Spazio Economico Europeo pari o superiore a 6,5 miliardi di euro negli ultimi tre esercizi finanziari, o se la capitalizzazione di mercato media o il valore equo di mercato equivalente dell’impresa cui appartiene era quanto meno pari a 65 miliardi di euro nell’ultimo esercizio finanziario, e se esso fornisce un servizio di piattaforma di base in almeno tre Stati membri.

Il secondo requisito si presume soddisfatto se viene fornito un servizio di piattaforma di base che annovera nell’ultimo esercizio finanziario più di 45 milioni di utenti finali attivi mensilmente, stabiliti o situati nell’Unione, e oltre 10.000 utenti commerciali attivi annualmente stabiliti nell’Unione.

Il terzo requisito consiste nel possedere i primi due requisiti in ciascuno degli ultimi tre esercizi finanziari.

Importante sottolineare che, nella proposta in commento, la competenza a stabilire se nel caso concreto un fornitore dei servizi di piattaforma di base sia qualificabile come *gatekeeper* spetta alla Commissione e che l’art. 3 del DMA fornisce non solo le suddette soglie che valgono come presunzioni di ricorrenza dei predetti requisiti, ma anche criteri qualitativi, nonché altri numerosi criteri di giudizio relativi alla struttura, la composizione e le caratteristiche dei mercati, al fine di guidare la decisione della Commissione. Gli artt. 3 e 4

stabiliscono i doveri di comunicazione alla Commissione cui sono tenuti i fornitori di servizi di piattaforma di base per consentire alla Commissione la sua valutazione, nonché alcune regole per la decisione e il riesame dello *status* di *gatekeeper*.

Il Capo III del DMA (artt. 5 ss.) prevede specifici obblighi, divieti e restrizioni posti in capo ai *gatekeeper* per impedire “pratiche sleali” o “pratiche che limitano la contendibilità”, attraverso un quadro normativo parzialmente flessibile: è prevista, infatti, la possibilità per la Commissione di aggiornare la struttura regolatoria a seguito di indagini di mercato.

Più nello specifico, il DMA di cui alla proposta in commento prevede divieti o restrizioni nell'esecuzione di determinate pratiche commerciali e prevede nuovi obblighi per favorire la concorrenza (artt. 6 e 7), oltre all'inserimento di rimedi *ad hoc* che si applicano sulla base di una analisi caso per caso. Tra i limiti imposti, bisogna evidenziare che si fa esplicito divieto di: a) usare i dati degli utenti commerciali al fine di competere con gli stessi; b) impedire agli utenti di accedere a servizi esterni alla piattaforma; c) impedire agli utenti di disinstallare qualsiasi *app* o *software* preinstallato sui propri dispositivi; d) garantire un trattamento più favorevole in termini di posizionamento ai servizi e prodotti offerti dalla piattaforma stessa (c.d. *self preferencing*) o da soggetti terzi appartenenti sempre al *gatekeeper*.

Il processo di verifica ed accertamento della qualifica di *gatekeeper* è seguito da un periodo di sei mesi in cui la piattaforma deve adeguarsi agli obblighi ed ai divieti imposti dal DMA. In caso di mancato adempimento degli obblighi imposti, sono previste sanzioni ed ammende per un importo fino al 10% del fatturato totale della piattaforma digitale (artt. 26 e ss.).

Come si legge nella proposta, l'obiettivo del DMA e dell'intera strategia digitale europea è quello di aumentare la coerenza e la certezza giuridica nell'ambiente delle piattaforme *online*, offrendo un quadro giuridico uniforme che superi i nazionalismi legislativi e che sappia prevenire i comportamenti sleali dei c.d. *gatekeeper*.

ENZO MARIA INCUTTI

<https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0842&from=en>

2021/1(5)RMo

### **Il parere del 10.02.2021 dello *European Data Protection Advisor* sulla proposta del *Digital Services Act* in particolare sulla pubblicità mirata e i *recommender systems***

Il 10 febbraio 2021 lo *European Data Protection Supervisor* (“EDPS”) ha espresso il proprio parere in merito alla proposta di Regolamento della Commissione europea relativa al *Digital Services Act* (la “**Proposta**”) su cui v. la notizia in questa rubrica *supra* [2021/1\(3\)ST](#).

L'EDPS constata innanzitutto la necessità di adottare adeguate misure di mitigazione dei rischi presenti nel contesto delle piattaforme *online*, segnalando in particolare i rischi connessi alla pubblicità mirata *online* ed all'impiego dei *recommender systems*.

Sul primo aspetto, l'Autorità giudica la Proposta idonea a garantire trasparenza ed *accountability* degli operatori di tali piattaforme. Ed infatti, l'EDPS osserva che la Proposta prevede (Articoli 24 e 30) che siano fornite al destinatario della pubblicità mirata informazioni circa i “*principali parametri*” usati per individuare i destinatari del messaggio pubblicitario e prescrive altresì che le piattaforme di notevoli dimensioni rendano accessibile al pubblico un repository contenente le suddette informazioni. L'EDPS, tuttavia, ritiene opportuno che si renda obbligatorio comunicare *ogni* parametro utilizzato, anziché i soli parametri principali, e

che, comunque, la Proposta chiarisca le condizioni minime necessarie affinché l'informazione da fornire sia “*meaningful*”, vale a dire idonea a trasmettere conoscenza. Preoccupazione evidente dell'EDPS è garantire che le nuove norme riescano a promuovere la consapevolezza del destinatario dell'informazione circa i rischi della pubblicità mirata (cfr. *EDPS's Guidelines 8/2020 on the targeting of social media users*, [https://edpb.europa.eu/sites/edpb/files/consultation/edpb\\_guidelines\\_202008\\_onthetargetingofsocialmediausers\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf), 5, 25).

Invece, con il fine di far sì che la pubblicità mirata non dia luogo a forme di discriminazione, l'Autorità suggerisce che l'articolo 30(2)(d) della Proposta, oltre a prescrivere che sia indicato se il messaggio pubblicitario è indirizzato ad uno o più gruppi *target*, chiarisca altresì quali gruppi sono esclusi e su quali criteri l'esclusione si basa.

Inoltre, secondo l'Autorità, andrebbero considerate salvaguardie ulteriori rispetto alla trasmissione di informazioni agli utenti. Tali misure dovrebbero includere restrizioni circa le categorie di dati che è consentito trattare a fini di pubblicità mirata e spingersi sino a prevedere la graduale messa al bando di quelle forme di pubblicità mirata, che abbiano luogo sulla base del tracciamento delle attività *online* dell'utente.

L'EDPS dedica, inoltre, particolare attenzione alla regolamentazione dei *recommender systems*, trattandosi di una tecnologia responsabile del preoccupante fenomeno noto come *'filter bubble'*. L'Autorità sottolinea che tali sistemi non si limitano a raccomandare contenuti (commerciali e non), ma più esattamente ‘curano’ i contenuti forniti agli utenti e dunque sono in grado di limitare la capacità di questi ultimi di ricercare ed interagire con le informazioni nell'ambiente *online*. Inoltre, tale attività è spesso svolta sulla base della profilazione degli utenti, con tutti i conseguenti rischi (segnalati dalla stessa EDPS, “*Opinion 3/2018 EDPS Opinion on online manipulation and personal data*”, 19 March 2018, p. 9, [https://edps.europa.eu/sites/edp/files/publication/18-03-19\\_online\\_manipulation\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf)).

Pertanto, in ossequio ai principi di protezione dei dati personali *by design* e *by default*, nonché del principio di minimizzazione, l'EDPS auspica che sia prescritta come impostazione *by default* che l'algoritmo di raccomandazione non si basi su dati di profilazione e che sia richiesto un esplicito *opting in* (anziché un *opting out*) dell'utente, al fine di rendere lecito un simile tipo di trattamento.

Inoltre, si raccomandano misure aggiuntive rispetto a quanto previsto dall'art. 29 della Proposta, atte a promuovere la trasparenza ed il controllo degli utenti in relazione ai sistemi di raccomandazione, tra cui: *i*) indicare chiaramente che la piattaforma utilizza un sistema di raccomandazione; *ii*) informare l'utente della piattaforma se il sistema di raccomandazione è un sistema decisionale automatizzato e, in tal caso, l'identità della persona fisica o giuridica responsabile della decisione; *iii*) consentire agli interessati di visualizzare il profilo od i profili relativi, utilizzati per curare il contenuto della piattaforma per il destinatario del servizio, nonché consentire a questi la cancellazione del o dei profili; *iv*) permettere ai destinatari del servizio di personalizzare i sistemi di raccomandazione sulla base di una serie di criteri (tempo, argomenti di interesse, etc.).

L'effettività di simili misure dipende dall'acquisita capacità dell'utente di conoscere la logica applicata da tali sistemi, nonché di comprenderne le implicazioni. In tale ottica, secondo l'EDPS, non può dirsi adeguata la disposizione, contenuta nell'Articolo 29 (1) della Proposta, con cui è resa obbligatoria la descrizione dei principali parametri impiegati dai *recommender systems*, da rendersi inserendo tale informazione all'interno dei termini e condizioni di servizio della piattaforma *online*.

L'EDPS accoglie con favore il fatto che la proposta si muova nel segno della integrazione della adottanda disciplina con le tutele di cui al regolamento (UE) 2016/679 e alla direttiva

2002/58/CE. In considerazione della incidenza degli aspetti da regolare sul trattamento dei dati personali, l'EDPS reputa necessario garantire la complementarità nella vigilanza e nel controllo delle piattaforme *online*, dando seguito all'esperienza e sviluppi relativi alla c.d. *Digital Clearinghouse* (cfr. *Opinion on coherent enforcement of fundamental rights in the age of Big Data*, 23 September 2016, [https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse\\_en](https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en)). A tal fine, tuttavia, l'EDPS stima opportuno che la Proposta preveda una base giuridica esplicita e completa per la cooperazione e lo scambio di informazioni pertinenti tra le diverse autorità di vigilanza.

ROBERTA MONTINARO

[https://edps.europa.eu/system/files/2021-02/21-02-10-opinion\\_on\\_digital\\_services\\_act\\_en.pdf](https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf)

2021/1(6)LC

### **La Risoluzione del 21.01.2021 del Parlamento europeo sul diritto dei lavoratori alla disconnessione**

Il 21 gennaio 2021 è stata approvata la Risoluzione del Parlamento europeo recante raccomandazioni alla Commissione sul diritto alla disconnessione (2019/2181(INL)), formalizzate in una proposta di direttiva (la “**Risoluzione**”). L’approvazione rappresenta il primo tentativo di definire a livello eurounitario il diritto alla disconnessione, inteso come diritto fondamentale dei lavoratori, da esercitare al di fuori dell’orario di lavoro senza incorrere in misure sfavorevoli da parte dei datori di lavoro.

La Risoluzione rientra nel quadro normativo già delineato da numerosi interventi europei in tema di salute e sicurezza sul lavoro. Ma il tema della disconnessione rappresenta una novità ed è strettamente connesso al fenomeno della digitalizzazione. Nella Risoluzione è espressa la consapevolezza che l’utilizzo sempre maggiore degli strumenti digitali a scopi lavorativi ha comportato la nascita di una cultura del “sempre connessi” che influisce negativamente sull’equilibrio tra vita professionale e vita privata dei lavoratori. Così, se da una parte l’utilizzo di strumenti digitali è stato determinante per tutelare posti di lavoro durante il confinamento per ragioni sanitarie, dall’altra gli orari di lavoro prolungati e le maggiori sollecitazioni sui lavoratori “da remoto” hanno fatto crescere i casi di ansia, *burnout* e altri disturbi psicofisici.

È quanto emerso dalle ricerche condotte da Eurofound (*European Foundation for the Improvement of Living and Working Conditions*), da cui prende le mosse la Risoluzione, secondo cui chi lavora da casa ha più del doppio delle probabilità di lavorare oltre le 48 ore settimanali massime previste rispetto a chi lavora in ufficio e quasi il 30% dei telelavoratori dichiara di lavorare nel proprio tempo libero, a fronte del 5% di coloro che lavorano in ufficio.

Analizzando più da vicino alcuni punti fondanti della Risoluzione, si segnala, ai sensi dell’art. 2, la definizione di “disconnessione” come “il mancato esercizio di attività o comunicazioni lavorative per mezzo di strumenti digitali, direttamente o indirettamente, al di fuori dell’orario di lavoro” e, come meglio specificato dal considerando 10, come “il diritto dei lavoratori di non svolgere mansioni o comunicazioni lavorative al di fuori dell’orario di lavoro per mezzo di strumenti digitali, come telefonate, email o altri messaggi”. Al fine di darne effettiva attuazione, la Risoluzione pone in capo agli Stati membri l’obbligo di stabilire, previa consultazione delle parti sociali, modalità dettagliate per consentire l’esercizio del

diritto alla disconnessione, tra cui modalità pratiche per scollegarsi dagli strumenti digitali a scopi lavorativi, compreso qualsiasi strumento di monitoraggio legato al lavoro (art. 4, co. 1, lett. a). Tra queste modalità di attuazione assume un rilievo centrale il sistema di misurazione dell'orario di lavoro (art. 4, co. 1, lett. b). Gli Stati membri dovranno, inoltre, assicurare che tale diritto sia effettivo, nel senso di garantire la tutela del lavoratore da qualsiasi tipo di trattamento sfavorevole da parte del datore di lavoro per non aver risposto a richieste lavorative al di fuori dell'orario lavorativo (art. 5), prevedendo un apposito regime sanzionatorio in caso di violazione delle disposizioni in materia (art. 8).

LUCIO CASALINI

[https://www.europarl.europa.eu/doceo/document/TA-9-2021-0021\\_IT.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2021-0021_IT.pdf)

2021/1(7)FR

### **Regolamento P2B e nuove funzioni delle Autorità indipendenti alla luce della Legge di Bilancio 2021**

La Legge di Bilancio 2021 (l. 30 dicembre 2020, n. 178, in vigore dal 1° gennaio 2021) contiene all'art. 1, commi 515-517, alcuni specifici riferimenti al “Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio del 20 giugno 2019 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione *online*” (il “**Regolamento**”).

Il Regolamento, che dal 12 luglio 2020 trova applicazione in tutta l'Unione europea, è diretto a disciplinare i rapporti *Platform-to-Business* (“**P2B**”), ovvero tra le imprese e, in senso ampio, le piattaforme digitali, in ciò rappresentando una significativa novità nel panorama normativo europeo in quanto, per la prima volta, si rivolge non ai consumatori, ma alle imprese quali nuovi soggetti deboli del mercato nel contesto della *platform economy*.

In primo luogo, il comma 515 modifica la l. 31 luglio 1997, n. 249, istitutiva dell'Autorità per le garanzie nelle comunicazioni (“**AGCOM**”), intervenendo sulle funzioni da essa attribuite a due degli organi collegiali dell'AGCOM: la Commissione per le infrastrutture e le reti, costituita dal Presidente e da due commissari; e il Consiglio, di cui fanno parte il Presidente e tutti i commissari. Rispetto alla Commissione, il riferimento è alla tenuta del Registro degli operatori di comunicazione (ROC), al cui interno è adesso altresì previsto che si iscrivano «i fornitori di servizi di intermediazione *on line* e i motori di ricerca *on line*, anche se non stabiliti, che offrono servizi in Italia» (art. 1, comma 6, lett. a), n. 5). Al Consiglio si attribuisce invece *ex novo* il compito di garantire l'adeguata ed efficace applicazione del Regolamento, «anche mediante l'adozione di linee guida, la promozione di codici di condotta e la raccolta di informazioni pertinenti» (art. 1, comma 6, lett. c), n. 14-bis). Peraltro, proprio l'adozione di codici di condotta è fortemente incoraggiata già dal legislatore europeo, soprattutto in relazione alla corretta applicazione dell'art. 5 del Regolamento in materia di *ranking*. La medesima disposizione estende inoltre la portata del successivo comma 31 dell'art. 1 della l. 249/1997, ove, anche per l'inottemperanza a quei provvedimenti che l'AGCOM abbia adottato a fronte della violazione delle norme del Regolamento, si prevede una sanzione amministrativa pecuniaria compresa tra il 2 e il 5 per cento del fatturato realizzato dal soggetto destinatario della contestazione nell'ultimo esercizio chiuso prima della sua notificazione.

A norma del comma 516, ai sensi del quale «[r]esta fermo quanto previsto dall'art. 27, comma 1-bis, del codice del consumo» (d. lgs. 6 settembre 2005, n. 206), appare poi volersi riconoscere all'Autorità garante della concorrenza e del mercato ("AGCM") la competenza a procedere, anche nell'ambito dei rapporti disciplinati dal Regolamento, nei confronti di condotte integranti pratiche commerciali scorrette.

Il comma 517 si riferisce infine alla copertura dei costi amministrativi sostenuti dall'AGCOM per l'esercizio delle sue funzioni e rinvia pertanto alla l. 23 dicembre 2005, n. 266, al cui art. 1 viene aggiunto il nuovo comma 66-bis. La nuova disposizione impone a carico dei fornitori di servizi di intermediazione e di motori di ricerca *online*, per l'anno 2021, una contribuzione pari all'1,5 per mille dei ricavi relativi al valore della produzione e realizzati nel territorio nazionale, a prescindere da dove vengano concretamente contabilizzati. Per gli anni successivi, competerà invece direttamente all'AGCOM l'individuazione di eventuali variazioni di tale rapporto, per quanto entro il valore massimo del 2 per mille di tali ricavi.

FEDERICO RUGGERI

[https://www.gazzettaufficiale.it/atto/serie\\_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2020-12-30&atto.codiceRedazionale=20G00202&elenco30giorni=false](https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2020-12-30&atto.codiceRedazionale=20G00202&elenco30giorni=false)

2021/1(8)CR

### **Clearview AI condannata in Germania per violazione del GDPR: il caso Marx**

Il 27 gennaio 2021 l'autorità per la protezione dei dati personali della città di Amburgo (l'"Autorità") ha ordinato alla società statunitense Clearview AI di cancellare i dati biometrici relativi ad un cittadino tedesco, Matthias Marx, acquisiti senza il consenso di quest'ultimo. La pronuncia è intervenuta in seguito al reclamo presentato dal Sig. Marx dopo che quest'ultimo aveva scoperto, esercitando il proprio diritto di accesso ex art. 13 GDPR, che Clearview AI deteneva a sua insaputa dati personali a lui relativi. Clearview AI è una società statunitense che acquisisce foto e video liberamente disponibili sul web (ad esempio da social *network* e *blog*) all'insaputa dei soggetti interessati e, attraverso un sistema di intelligenza artificiale, estrae i profili biometrici delle persone raffigurate che vengono poi conservati all'interno di un database. Tale tecnologia permette di associare rapidamente il volto di qualunque persona a milioni di immagini, riuscendo così a ricostruirne l'identità. In particolare, le forze dell'ordine statunitensi si avvalgono di tale sistema per poter identificare persone di interesse di cui non si hanno sufficienti informazioni.

Clearview AI si è difesa sostenendo di non essere soggetta agli obblighi imposti dal GDPR essendo una società con sede negli Stati Uniti e priva di uno stabilimento all'interno dell'UE. L'Autorità, tuttavia, ha rigettato tale opposizione sulla base del fatto che il Regolamento, ai sensi dell'art. 3(2)(b), si applica a tutti i trattamenti di dati personali relativi a soggetti che si trovano nell'Unione, indipendentemente dal luogo della sede del titolare del trattamento, quando il trattamento consiste nel monitoraggio del comportamento degli interessati. Nel caso in esame, l'Autorità ha precisato che il trattamento svolto da Clearview AI costituisce un monitoraggio in quanto è finalizzato ad identificare le persone attraverso la loro profilazione.

Alla luce di ciò, l'Autorità ha riconosciuto che Clearview AI è soggetta all'obbligo di individuare una valida base giuridica per il trattamento dei dati personali tra quelle di cui agli

art. 6 o 9 GDPR. Nello specifico, essendo i dati biometrici inclusi tra le categorie particolari di dati personali, il trattamento deve essere fondato su una delle basi individuate dall'art. 9 GDPR. Nel caso concreto, la base giuridica più idonea è stata individuata dall'Autorità nel consenso dell'interessato che, tuttavia, non è stato acquisito da Clearview AI. Pertanto, il trattamento risulta invalido e, sulla base dell'art. 17 GDPR che riconosce il diritto alla cancellazione, l'Autorità ha ordinato al titolare di cancellare i dati biometrici relativi al Sig. Marx.

Tale decisione risulta tuttavia limitata sotto due profili. In primo luogo, l'Autorità ha disposto la cancellazione solo per i dati relativi al Sig. Marx, con la conseguenza che altri cittadini europei le cui foto siano state inserite (senza il loro consenso) nel database di Clearview AI, dovranno personalmente presentare una apposita richiesta di cancellazione al titolare del trattamento e, eventualmente, un reclamo all'autorità per la protezione dei dati personali del loro Stato di residenza. In secondo luogo, l'Autorità ha ordinato solamente la cancellazione degli *hash*, ovvero i codici numerici che permettono di estrarre da una fotografia i dati biometrici delle persone raffigurate e di creare un profilo biometrico. Al contrario, non è stata disposta l'eliminazione delle singole foto.

CHIARA RAUCCIO

[https://noyb.eu/sites/default/files/2021-01/545\\_2020\\_Anhörung\\_CVAI\\_ENG\\_Redacted.PDF](https://noyb.eu/sites/default/files/2021-01/545_2020_Anhörung_CVAI_ENG_Redacted.PDF)

2021/1(9)CM

### **Apple condannata dal Tribunale di Milano a fornire accesso al patrimonio digitale di un defunto (ordinanza del 09.02.2021)**

Con un provvedimento emesso in data 9 febbraio 2021, il Tribunale di Milano, Prima Sezione Civile, si è pronunciato in materia di accesso al patrimonio digitale di un defunto.

Per la prima volta in Italia, a quanto consta, un giudice ha ordinato in via cautelare d'urgenza ad una società del gruppo Apple (la Apple S.r.l., di seguito “**Apple**”) di fornire la propria assistenza ai genitori di un ragazzo deceduto al fine di consentire il recupero dei dati dell'*account i-cloud* del figlio. Nel caso di specie, il ragazzo era deceduto in un incidente stradale e l'assistenza di Apple risultava necessaria in quanto il suo *smartphone* era andato distrutto nell'incidente.

Leggendo la motivazione del provvedimento (l’“**Ordinanza**”) si apprende che, alla richiesta dei genitori di accedere alle credenziali dell'*account* del figlio, Apple aveva risposto affermando che avrebbe consentito loro l'accesso ai dati contenuti dell'ID Apple solo a fronte di un ordine di un Tribunale avente determinati contenuti, alcuni dei quali peraltro anche estranei all'ordinamento giuridico italiano (poiché facenti riferimento a quello americano).

Il 14.12.2020 i genitori proponevano pertanto ricorso *ex artt. 669-bis e 700 c.p.c.* al Tribunale di Milano chiedendo, in via cautelare, di emettere, con decreto *inaudita altera parte*, o con ordinanza, previa audizione delle parti, i provvedimenti necessari ed idonei a tutelare i diritti dei ricorrenti e, segnatamente, chiedendo di ordinare alla Apple di fornire assistenza nel recupero dei dati personali dagli *account* del figlio defunto.

Apple non si costituiva in giudizio e rimaneva pertanto contumace.

A fondamento della domanda cautelare, i genitori affermavano, da una parte, il *fumus*, ravvisabile nella ricorrenza *prima facie* dei requisiti di applicabilità della norma di cui all'articolo 2-terdecies del nuovo Codice in materia di dati personali (il “**Codice privacy**”), dall'altra, il *periculum*, consistente nel fatto che la società di Cupertino aveva comunicato ai genitori che i propri sistemi, dopo un periodo di inattività dell'*account i-cloud*, avrebbero automaticamente distrutto i dati dello stesso *account*.

La norma di cui all'articolo 2-terdecies co. 1 del Codice Privacy dispone che i diritti relativi ai dati personali delle persone decedute possono essere esercitati “da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione”. Pertanto, volendo i genitori accedere ai dati del figlio contenuti nel *cloud* al fine di “poter cercare di colmare – almeno in parte – quel senso di vuoto e l'immenso dolore che si accompagna alla prematura perdita di un proprio caro”, il Tribunale riteneva che questo caso integrasse pienamente l'ipotesi delle “ragioni familiari meritevoli di protezione” richieste dalla norma e, ricorrendo inoltre il requisito del *periculum* per la ragione rappresentata dai ricorrenti, giudicava fondato il ricorso ed emetteva l'ordine richiesto dai ricorrenti.

La pronuncia risulta particolarmente interessante posto che il GDPR (reg. UE n. 2016/679) non contiene disposizioni in materia, ed anzi il Considerando 27 del GDPR dispone espressamente che il medesimo regolamento “non si applica ai dati personali delle persone decedute”, aggiungendo subito dopo che “[g]li Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute”.

Viceversa, l'art. 2-terdecies del Codice privacy, introdotto con il decreto legislativo 10 agosto 2018, n. 101 e rubricato “Diritti riguardanti le persone decedute”, contiene, come sopra ricordato, una nuova disposizione specificamente dedicata al tema della tutela *post-mortem* e dell'accesso ai dati personali del defunto, che, al comma 1, così reca: “I diritti di cui agli articoli da 15 a 22 del Regolamento [GDPR] riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione”.

Nell'Ordinanza, il Tribunale di Milano osserva che, come già per la previgente disciplina, il legislatore italiano non chiarisce qui se si tratti di un acquisto *mortis causa* o di una legittimazione *iure proprio*, “limitandosi a prevedere quello che la più attenta dottrina ha qualificato in termini di ‘persistenza’ dei diritti oltre la vita della persona fisica (diritti che prevedono il diritto di accesso, di rettifica, di limitazione di trattamento, di opposizione, ma anche il diritto alla cancellazione ed alla portabilità dei dati), persistenza che assume rilievo preminente a livello dei rimedi esperibili”. Da qui la ricostruzione per la quale i diritti dell'interessato “sopravvivono” alla sua morte ed essi possono essere esercitati da determinati soggetti “legittimati”. Dopo una digressione sul contenuto dei successivi commi del medesimo art. 2-terdecies del Codice privacy (non rilevanti per la decisione del caso), il Tribunale ha affrontato la questione dei “requisiti” di contenuto, che, ai termini delle condizioni generali del contratto di servizio predisposte da Apple, un ipotetico ordine del tribunale dovrebbe presentare per consentire ad Apple di fornire l'assistenza e l'accesso ai dati. In particolare, nelle comunicazioni inviate da Apple ai genitori del ragazzo defunto si richiedeva: “un ordine del tribunale che specifichi: 1) che il defunto era il proprietario di tutti gli *account* associati all'ID Apple; 2) che il richiedente è l'amministratore o il rappresentante legale del patrimonio del defunto; 3) che, in qualità di amministratore o rappresentante legale, il richiedente agisce come ‘agente’ del defunto e la sua autorizzazione costituisce un ‘consenso legittimo’, secondo le definizioni date nell'Electronic Communications Privacy Act; 4) che il tribunale ordina a Apple di fornire assistenza nel recupero dei dati personali dagli *account* del defunto, che potrebbero contenere anche informazioni o dati personali

identificabili di terzi”. Con riferimento a tali richieste il Tribunale di Milano, nell’Ordinanza osservava quanto segue: “solo Apple è a conoscenza delle informazioni relative al punto 1); nell’ordinamento italiano non esiste la figura dell’ ‘amministratore o rappresentante legale del patrimonio del defunto’ né, tantomeno, quello di ‘agente’ del *de cuius*; la disciplina legislativa italiana non richiede, in alcun modo, né l’autorizzazione di un ‘agente’ del defunto all’accesso né la presenza di un ‘consenso legittimo’ secondo un atto normativo di un ordinamento giuridico diverso”.

Sulla base di queste osservazioni, il Tribunale di Milano ha definito “del tutto illegittima la pretesa avanzata dalla società resistente di subordinare l’esercizio di un diritto, riconosciuto dall’ordinamento giuridico italiano, alla previsione di requisiti del tutto estranei alle norme di legge che disciplinano la fattispecie in esame”.

Infine, e “solo per completezza”, il Tribunale di Milano ha osservato che, relativamente alla questione dell’applicabilità del GDPR a tutela della posizione di Apple che aveva motivato la sua resistenza invocando la “sicurezza dei clienti”, viene in evidenza l’art. 6, par. 1, lettera f) del medesimo regolamento, che autorizza il trattamento dei dati personali necessario per il “perseguimento del legittimo interesse” del titolare o di terzi. Pertanto, avendo preso atto che i ricorrenti avevano chiesto di accedere agli *account* personali del defunto figlio per “ragioni familiari meritevoli di protezione”, il Tribunale ha stabilito che dovesse ritenersi sussistente il predetto legittimo interesse anche ai fini dell’applicazione dell’art. 6, par. 1, lettera f) del GDPR.

CORRADO MORICONI

[https://web.uniroma1.it/deap/sites/default/files/allegati/Trib\\_Milano\\_Apple\\_credita\\_digitale\\_9\\_feb\\_2021.pdf](https://web.uniroma1.it/deap/sites/default/files/allegati/Trib_Milano_Apple_credita_digitale_9_feb_2021.pdf)

2021/2(1)SO

### **Verso l’*Artificial Intelligence Act*: la Proposta di Regolamento del 21.04.2021 su regole armonizzate in materia di intelligenza artificiale.**

Con il documento COM(2021) 206 final del 21 aprile 2021, recante “Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull’intelligenza artificiale (legge sull’intelligenza artificiale) e modifica alcuni atti legislativi dell’unione”, la Commissione europea ha pubblicato una proposta normativa volta a fissare un quadro di divieti e di requisiti per i sistemi di IA, comprensivo di un apparato sanzionatorio e istituzionale (la “**Proposta di *AI Act***”).

La Proposta di *AI Act* comprende una bozza di regolamento (la “**Bozza di Regolamento**”) con i relativi allegati (gli “**Allegati**”) ed una relazione esplicativa (la “**Relazione**”).

Nella Relazione si ricordano innanzitutto i principali documenti e le principali azioni adottate negli ultimi anni dalle istituzioni dell’Unione europea in materia di intelligenza artificiale (“**IA**”). In particolare, per quanto riguarda il Consiglio europeo, la Relazione ricorda: lo *European Council meeting (19 October 2017) – Conclusion* EUCO 14/17, 2017, p. 8; l’*Artificial intelligence b) Conclusions on the coordinated plan on artificial intelligence-Adoption* 6177/19, 2019; lo *Special meeting of the European Council (1 and 2 October 2020) – Conclusions*, EUCO 13/20, 2020, p. 6; le *Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, 11481/20, 2020.

Quanto al Parlamento europeo, la Relazione ricorda le risoluzioni adottate nell'ottobre 2020 sull'etica, la responsabilità civile e il *copyright* (preceduti dalla pubblicazione di tre *draft reports* della commissione JURI dell'aprile 2020, sui quali v. le notizie [2020/2\(2\)CR](#), [2020/2\(3\)SO](#) e [2020/2\(4\)LC](#)): la *European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies*, 2020/2012(INL); la *European Parliament resolution of 20 October 2020 on a civil liability regime for artificial intelligence*, 2020/2014(INL) (su cui la notizia [2020/4\(1\)SG](#)), la *European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies*, 2020/2015(INI); nonché i documenti del 2021 in materia di diritto penale e in materia di educazione, cultura e settore audiovisivo: lo *European Parliament Draft Report, Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*, 2020/2016(INI) e lo *European Parliament Draft Report, Artificial intelligence in education, culture and the audiovisual sector*, 2020/2017(INI).

Quanto alla Commissione europea, la Relazione ricorda il libro bianco sulla IA del febbraio 2020, ossia lo *European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust*, COM(2020) 65 final, 2020 (su cui v. la notizia [2020/1\(5\)SO](#)), nonché il *Digital Education Action Plan 2021-2027: Resetting education and training for the digital age, which foresees the development of ethical guidelines in AI and Data usage in education* – Commission Communication COM(2020) 624 final.

La Relazione spiega che la Bozza di Regolamento è stata concepita con l'intenzione di limitare i requisiti legali per le imprese che immettono soluzioni di IA nel mercato nella misura minima necessaria per affrontare i “rischi” e i “problemi” legati all'IA. Nella Relazione si dà atto che, in esito ad una consultazione pubblica, l'opzione scelta per la Bozza di Regolamento riflette il modello di uno strumento legislativo “orizzontale” che segue un approccio proporzionato basato sul rischio, e che contempla codici di condotta per i sistemi di IA “non ad alto rischio”. In conseguenza della scelta di modello legislativo “orizzontale”, la Proposta di *AI Act* è intesa ad inserirsi in un quadro normativo coerente avuto riguardo alle altre normative e politiche legislative dell'Unione e viene specificato che la Proposta di *AI Act* non pregiudica l'applicazione del diritto della concorrenza dell'Unione. La Bozza di Regolamento è dichiaratamente coerente con la Carta dei diritti fondamentali della UE e l'esistente legislazione “secondaria” dell'Unione sulla protezione dei dati personali, sulla tutela dei consumatori, sulla non discriminazione e sull'uguaglianza di genere. In particolare, la Relazione specifica che la Proposta di *AI Act* non pregiudica bensì integra le disposizioni del GDPR (Regolamento (UE) 2016/679) e della direttiva *Law Enforcement* (Direttiva (UE) 2016/680) prevedendo regole armonizzate sulla progettazione, sviluppo e uso di certi sistemi di IA ad alto rischio e alcuni limiti per alcune utilizzazioni di sistemi di identificazione biometrica a distanza. La Relazione dichiara che la Bozza di Regolamento si propone di integrare la legislazione esistente dell'Unione sulla non-discriminazione al fine di minimizzare il rischio di “discriminazione algoritmica”. Con riferimento ai sistemi di IA ad alto rischio relativi a prodotti disciplinati dalla legislazione del c.d. “Nuovo Quadro Normativo” (*New Legislative Framework*, “NLF”), ad es. macchinari, dispositivi medici, giocattoli, etc., la Relazione specifica che i requisiti per i sistemi di IA previsti nella Bozza di Regolamento dovranno essere controllati nel contesto delle procedure di controllo di conformità previsti dalla legislazione NLF di volta in volta applicabile. Per quanto riguarda la questione del coordinamento tra i vari e diversi requisiti, la Relazione precisa che mentre la Bozza di Regolamento intende occuparsi dei rischi di sicurezza tipici dei sistemi di IA attraverso la predisposizione di specifici requisiti, la legislazione NLF è intesa ad assicurare la sicurezza complessiva del prodotto finale e può, di conseguenza, contenere la previsione di specifici requisiti che riguardano condizioni per integrare in modo sicuro un sistema di IA in un

prodotto finale. A questo riguardo, la Relazione aggiunge che tale approccio è seguito dalla **proposta di Machinery Regulation** adottata il 21 aprile 2021, ossia nello stesso giorno della Proposta di *LA Act: Proposal for a Regulation of the European Parliament and of the Council on machinery products* COM(2021) 202 (<https://ec.europa.eu/docsroom/documents/45508>).

Nell'Allegato II, sezione A della Bozza di Regolamento, sono elencati i seguenti atti della legislazione NLF: Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la direttiva 95/16/CE [che si prevede sarà abrogata dal nuovo regolamento sui prodotti macchina]; Direttiva 2009/48/CE del Parlamento europeo e del Consiglio, del 18 giugno 2009, sulla sicurezza dei giocattoli; Direttiva 2013/53/UE del Parlamento europeo e del Consiglio, del 20 novembre 2013, relativa alle imbarcazioni da diporto e alle moto d'acqua e che abroga la direttiva 94/25/CE; Direttiva 2014/33/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, per l'armonizzazione delle legislazioni degli Stati membri relative agli ascensori e ai componenti di sicurezza per ascensori; Direttiva 2014/34/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative agli apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva; Direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE; Direttiva 2014/68/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di attrezzature a pressione; Regolamento (UE) 2016/424 del Parlamento europeo e del Consiglio, del 9 marzo 2016, relativo agli impianti a fune e che abroga la direttiva 2000/9/CE; Regolamento (UE) 2016/425 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sui dispositivi di protezione individuale e che abroga la direttiva 89/686/CEE del Consiglio; Regolamento (UE) 2016/426 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sugli apparecchi che bruciano carburanti gassosi e che abroga la direttiva 2009/142/CE; Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio; Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione.

Invece, per quanto riguarda i sistemi di IA ad alto rischio relativi a prodotti disciplinati dalla legislazione del c.d. vecchio approccio ("**Old Approach legislation**"), ad es. aeromobili, autoveicoli, la Relazione aggiunge che la Proposta di *AI Act* non si applica direttamente, e che, tuttavia, gli essenziali requisiti *ex-ante* per i sistemi di IA di alto rischio dovranno essere presi in considerazione quando si adotteranno normative attuative o delegate della medesima legislazione. Ciò è ribadito nel Considerando 29 e nell'art. 2, para. 2 della Bozza di Regolamento, relativamente ai seguenti atti della c.d. *Old Approach legislation*: Regolamento (CE) 300/2008 che istituisce norme comuni per la sicurezza dell'aviazione civile; Regolamento (UE) No 167/2013 sull'omologazione e la vigilanza del mercato dei veicoli agricoli e forestali; Regolamento (UE) No 168/2013 sull'omologazione e la vigilanza del mercato dei veicoli a motore a due o tre ruote e dei quadricicli; Direttiva 2014/90/UE sull'equipaggiamento marittimo; Direttiva (UE) 2016/797 sull'interoperabilità del sistema ferroviario dell'Unione europea; Regolamento (UE) 2018/858 sull'omologazione e la vigilanza del mercato dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, dei componenti e delle entità tecniche indipendenti destinati a tali veicoli; Regolamento (UE)

2018/1139 recante norme comuni nel settore dell'aviazione civile e che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea; Regolamento (UE) 2019/2144 sui requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada. Riferendosi a tali atti, il Considerando 29 della Bozza di Regolamento statuisce che è opportuno modificarli per far sì che la Commissione, nell'adottare qualsiasi futuro provvedimento attuativo o delegato sulla base dei medesimi atti, possa tener conto dei requisiti obbligatori *ex-ante* stabiliti nella Bozza di Regolamento per i sistemi di IA ad alto rischio, sulla base delle specificità tecniche e regolamentari di ciascun settore; e l'art. 2 para 2 della Bozza di Regolamento prevede che ai sistemi di IA ad alto rischio che costituiscono componenti di sicurezza di prodotti o sistemi, o che sono essi stessi prodotti o sistemi disciplinati dagli atti di cui sopra, si applica soltanto l'art. 84 della Bozza di Regolamento, il quale ultimo prevede alcuni compiti della Commissione in materia di revisione della normativa.

La Relazione aggiunge che per quanto concerne i sistemi di IA forniti o utilizzati da enti creditizi regolamentati, le autorità competenti per il controllo sulla legislazione dell'Unione in materia di servizi finanziari dovrebbero essere designate come autorità competenti per il controllo dell'osservanza dei requisiti previsti dalla Proposta di *AI Act* al fine di assicurare un'applicazione coerente della normativa dell'Unione in materia di servizi finanziari laddove i sistemi di IA siano in una certa misura implicitamente regolamentati in relazione al sistema di *governance* interna degli enti creditizi. A tal proposito, l'art. 9, ultimo paragrafo della Bozza di Regolamento prevede che per gli enti creditizi disciplinati dalla direttiva 2013/36/UE (la direttiva sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale) le previsioni dettate dal medesimo art. 9 della Bozza di Regolamento in materia di gestione dei rischi si debbano osservare includendole nelle procedure di gestione dei rischi previste dalla medesima direttiva. Infine, la Relazione dichiara che la Proposta di *AI Act* è coerente con la legislazione dell'Unione applicabile ai servizi, compresi i servizi di intermediazione regolati dalla direttiva sul commercio elettronico (direttiva 2000/31/CE) e la recente proposta della Commissione per la legge sui servizi digitali, c.d. *Digital Services Act* (su cui v. notizia [2021/1\(3\)ST](#)). Per quanto riguarda le altre linee di politica legislativa dell'Unione, la Relazione sottolinea la coerenza della Proposta di *AI Act* con i documenti in materia di innovazione digitale (Comunicazione della Commissione, “Plasmare il futuro digitale dell'Europa” (COM(2020) 67 final; “Bussola per il digitale 2030: il modello europeo per il decennio digitale”) e in materia di *governance* e mercato dei dati (Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla *governance* europea dei dati (c.d. *Data Governance Act*) (COM/2020/767); Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico; Comunicazione della Commissione, “Una strategia europea per i dati” (COM/2020/66 final)).

La Relazione specifica che la base dell'intervento è ravvisata nell'art. 114 TFUE, e richiama i principi di sussidiarietà e di proporzionalità. Sempre secondo la Relazione, la Bozza di Regolamento persegue i seguenti obiettivi:

- assicurare che i sistemi di IA immessi e utilizzati nel mercato dell'Unione siano sicuri e rispettino la normativa esistente sui diritti fondamentali e i valori dell'Unione;
- assicurare certezza del diritto al fine di facilitare l'investimento e l'innovazione in IA;
- rafforzare l'effettiva applicazione della normativa esistente sui diritti fondamentali e sui requisiti di sicurezza applicabili ai sistemi di IA;
- facilitare lo sviluppo di un mercato unico per applicazioni di IA legittime, sicure e meritevoli di fiducia ed evitare la frammentazione di mercato.

Venendo ai contenuti della Bozza di Regolamento, il titolo I (artt. 1-4) definisce l'oggetto del regolamento e l'ambito di applicazione delle nuove regole concernenti l'immissione sul mercato, la messa in servizio e l'utilizzo di sistemi di IA. L'art. 2 para. 1 stabilisce che la Bozza di Regolamento si applica: a) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA nell'Unione, indipendentemente dal fatto che siano stabiliti nell'Unione o in un paese terzo; b) agli utenti dei sistemi di IA situati nell'Unione; c) ai fornitori e agli utenti di sistemi di IA situati in un paese terzo, laddove l'*output* prodotto dal sistema sia utilizzato nell'Unione. L'art. 2 para. 3 prevede che la Bozza di Regolamento non si applica ai sistemi di IA sviluppati o usati per scopi esclusivamente militari. L'art. 2 para. 4 esclude l'applicazione del regolamento alle “*autorità pubbliche di un paese terzo [e] alle organizzazioni internazionali [...], laddove tali autorità o organizzazioni utilizzino i sistemi di IA nel quadro di accordi internazionali per la cooperazione delle autorità di contrasto e giudiziarie con l'Unione o con uno o più Stati membri*”. L'art. 3 della Bozza di Regolamento stabilisce le definizioni utilizzate in tutto l'atto. Come si ricava anche dalla Relazione, la definizione di sistema di IA intende essere “*future proof*” ossia mira ad essere il più possibile neutrale dal punto di vista tecnologico e in questo senso adeguata alle esigenze future. Il sistema di IA è definito come “*un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono*”. L'Allegato I della Bozza di Regolamento prevede le seguenti tre tipologie di “*approcci*” e “*tecniche*” in funzione della predetta definizione: “*a) Approcci di apprendimento automatico [machine learning], compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (deep learning); b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenza, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti; c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione.*”. È previsto che tale allegato debba essere adattato dalla Commissione in linea con i nuovi sviluppi tecnologici. L'art. 3 definisce anche gli “*operatori*” lungo l'intera catena del valore dell'IA, ossia il “*fornitore*” (e anche il “*fornitore di piccole dimensioni*”), l’“*utente*”, il “*rappresentante autorizzato*”, l’“*importatore*” e il “*distributore*”, considerando tanto gli operatori pubblici quanto quelli privati.

Il titolo II della Bozza di Regolamento – che consiste del solo articolo 5 – prevede quattro fattispecie di “*pratiche*” di IA vietate. In modo conforme a molti atti e documenti in materia, la Bozza di Regolamento segue un approccio basato sul rischio, differenziando tra gli usi dell'IA che creano: i) un rischio inaccettabile; ii) un rischio alto; iii) un rischio basso o minimo. Le “*pratiche*” vietate di cui all'art. 5 sono quelle che secondo la Bozza di Regolamento creano un rischio inaccettabile. Relativamente alle prime tre fattispecie di cui all'art. 5 per “*pratiche*” si intendono “*l'immissione sul mercato, la messa in servizio o l'uso*” di un sistema di IA, mentre per la quarta fattispecie, la pratica vietata è il solo “*uso*”. Le prime due fattispecie di pratiche riguardano sistemi di IA idonei a falsare il comportamento delle persone in modo tale da procurare un “*danno fisico o psicologico*”. La terza fattispecie riguarda sistemi di IA di c.d. *social scoring* e il divieto si applica solo se le pratiche sono poste in essere da autorità pubbliche o per loro conto e se tali sistemi di AI sono idonei a produrre determinati “*trattamenti pregiudizievole o sfavorevoli*” per determinate persone o gruppi di persone. La quarta fattispecie di pratica vietata consiste nell'uso di sistemi di IA di identificazione biometrica remota “*in tempo reale*” in spazi accessibili al pubblico a fini di attività di contrasto svolte dalle autorità per la prevenzione, indagine, accertamento o perseguimento di reati o per esecuzione di sanzioni penali, fatta salva l'applicazione di talune eccezioni limitate.

Il titolo III della Bozza di Regolamento (artt. 6-51) contiene regole specifiche per i sistemi di IA che creano un “*rischio alto*” per la salute e la sicurezza o per i diritti fondamentali delle

persone fisiche. In linea con un approccio basato sul rischio, tali sistemi di IA ad alto rischio sono consentiti sul mercato europeo subordinatamente al rispetto di determinati requisiti obbligatori e ad una valutazione della conformità *ex ante*. La classificazione di un sistema di IA come ad alto rischio si basa sulla sua finalità prevista, in linea con la normativa vigente dell'UE in materia di sicurezza dei prodotti. Di conseguenza la classificazione come ad alto rischio non dipende solo dalla funzione svolta dal sistema di IA, ma anche dalle finalità e modalità specifiche di utilizzo di tale sistema.

Il capo 1 del titolo III fissa le regole di classificazione e individua nell'art. 6 due categorie principali di sistemi di IA ad alto rischio:

- i sistemi di IA destinati ad essere utilizzati come componenti di sicurezza di prodotti, o che sono essi stessi prodotti, soggetti a valutazione di conformità *ex ante* da parte di terzi, ai sensi della normativa di armonizzazione dell'Unione di cui all'Allegato II;
- altri sistemi di IA c.d. "indipendenti" che presentano implicazioni principalmente in relazione ai diritti fondamentali esplicitamente elencati nell'Allegato III.

Tale elenco di sistemi di IA ad alto rischio di cui all'Allegato III contiene una descrizione tipologica di 21 sistemi di IA afferenti ai seguenti 8 settori, dichiaratamente scelti dalla Commissione ed inseriti nel medesimo Allegato III per la circostanza che i relativi "rischi" si sono già "concretizzati" o "potrebbero concretizzarsi nel prossimo futuro": (i) Identificazione e categorizzazione biometrica delle persone fisiche; (ii) Gestione e funzionamento delle infrastrutture critiche; (iii) Istruzione e formazione professionale; (iv) Occupazione, gestione dei lavoratori e accesso al lavoro autonomo; (v) Accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi; (vi) Attività di contrasto di reati; (vii) Gestione della migrazione, dell'asilo e del controllo delle frontiere; (viii) Amministrazione della giustizia e processi democratici. Al fine di assicurare che il regolamento possa essere adattato in futuro agli usi e alle applicazioni emergenti dell'intelligenza artificiale, è previsto che la Commissione possa ampliare l'elenco dei sistemi di IA ad alto rischio utilizzati all'interno di alcuni settori predefiniti, applicando una serie di criteri e una metodologia di valutazione dei rischi.

Il capo 2 del titolo III definisce i requisiti giuridici per i sistemi di IA ad alto rischio in relazione a dati e *governance* dei dati (art. 10), documentazione (art. 11 e Allegato IV) e conservazione delle registrazioni, trasparenza e fornitura di informazioni agli utenti, sorveglianza umana, robustezza, accuratezza e sicurezza.

Il capo 3 del titolo III definisce una serie di obblighi orizzontali per i fornitori di sistemi di IA ad alto rischio. Obblighi proporzionati sono imposti anche a utenti e altri operatori.

Il capo 4 del titolo III definisce il quadro per gli organismi notificati che saranno coinvolti come terze parti indipendenti nelle procedure di valutazione della conformità, mentre il capo 5 del titolo III prevede le procedure di valutazione della conformità da seguire per ciascun tipo di sistema di IA ad alto rischio. A tali procedure si riferiscono gli Allegati V, VI, VII e VIII.

Il titolo IV della Bozza di Regolamento, che consiste del solo art. 52, prevede "obblighi di trasparenza" per i sistemi di IA che: i) interagiscono con gli esseri umani; ii) sono utilizzati per rilevare emozioni o stabilire un'associazione con categorie (sociali) sulla base di dati biometrici; oppure iii) generano o manipolano contenuti ("*deep fake*"). È previsto che le persone debbano essere informate quando interagiscono con un sistema di IA o le loro emozioni o caratteristiche vengono riconosciute attraverso mezzi automatizzati. Se un sistema di IA viene utilizzato per generare o manipolare immagini o contenuti audio o video che assomigliano notevolmente a contenuti autentici, è previsto in linea generale, e salve alcune eccezioni per finalità legittime (come la finalità di contrasto di reati e la libertà di

espressione), l'obbligo di rivelare che tali contenuti sono generati ricorrendo a mezzi automatizzati.

Il titolo V della Bozza di Regolamento (artt. 53-55) dedicato alle “misure di sostegno all'innovazione” prevede alcune disposizioni in materia di spazi di sperimentazione normativa, le c.d. *sand-boxes*.

Il titolo VI della Bozza di Regolamento (artt. 56-59) dedicato alla “*governance*” prevede il quadro istituzionale per i sistemi di IA, ed in particolare l'istituzione di un Comitato europeo per l'IA (lo “*European Artificial Intelligence Board*”), costituito da rappresentanti degli Stati membri e della Commissione europea. A livello nazionale, è previsto che gli Stati membri dovranno designare una o più autorità nazionali competenti e, tra queste, l'autorità nazionale di controllo, al fine di controllare l'applicazione e l'attuazione del regolamento.

Il titolo VII della Bozza di Regolamento, che consiste del solo art. 60, intitolato “Banca dati dell'UE per i sistemi di IA indipendenti ad alto rischio” prevede la creazione di una banca dati a livello dell'UE per sistemi di IA ad alto rischio “indipendenti” che presentano principalmente implicazioni in relazione ai diritti fondamentali. È previsto che la banca dati sia gestita dalla Commissione e alimentata con i dati messi a disposizione dai fornitori dei sistemi di IA, che saranno tenuti a registrare i propri sistemi prima di immetterli sul mercato o altrimenti metterli in servizio.

Il titolo VIII della Bozza di Regolamento (artt. 61-68) intitolato “Monitoraggio successivo all'immissione sul mercato, condivisione delle informazioni, vigilanza del mercato” stabilisce gli obblighi in materia di monitoraggio e segnalazione per i fornitori di sistemi di IA per quanto riguarda il monitoraggio successivo all'immissione sul mercato e la segnalazione di incidenti e malfunzionamenti correlati all'IA nonché le indagini in merito. È previsto che il regolamento (UE) 2019/1020 sulla vigilanza dei mercati e sulla conformità dei prodotti si applichi ai sistemi di IA disciplinati dalla Bozza di Regolamento.

Il titolo IX della Bozza di Regolamento, che consiste del solo art. 69, intitolato “Codici di condotta” mira a incoraggiare i fornitori di sistemi di IA non ad alto rischio ad applicare volontariamente i requisiti obbligatori previsti per i sistemi di IA ad alto rischio

Il titolo X della Bozza di Regolamento (artt. 70-73) intitolato “Riservatezza e sanzioni” contiene alcune importanti disposizioni, in particolare l'art. 71 che prevede sanzioni amministrative pecuniarie per la violazione del divieto di cui all'art. 5 (pratiche vietate) e la mancata osservanza dei requisiti di conformità di cui all'art. 10 (dati e *governance* dei dati) nella misura di un importo fino a 30 milioni di euro o, in caso di società, di un importo fino al 6 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Sanzioni amministrative pecuniarie con tetti massimi inferiori sono previste per l'inosservanza di altre disposizioni della Bozza di regolamento, diverse da quelle contenute negli artt. 5 e 10. L'art. 72 prevede sanzioni amministrative pecuniarie a carico di istituzioni, agenzie e organismi dell'Unione. L'art. 70 prevede che le autorità nazionali competenti e gli organismi notificati che partecipano all'applicazione del regolamento debbano rispettare la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività in modo da tutelare, *inter alia*, i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali di una persona fisica o giuridica, compreso il codice sorgente, salva l'applicazione dell'art. 5 della direttiva 2016/943 sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali). L'art. 70 contiene altre previsioni in materia di scambio di informazioni tra le autorità competenti.

I restanti titoli XI e XII contengono le regole per l'esercizio della delega e delle competenze di esecuzione e alcune disposizioni finali, tra cui la previsione dell'esclusione di applicazione del regolamento ai sistemi di IA che sono componenti di “sistemi IT su larga scala” come istituiti dagli atti giuridici elencati nell'Allegato IX, che siano stati immessi sul

mercato o messi in servizio in un periodo antecedente alla futura entrata in vigore del regolamento. L'Allegato IX elenca la legislazione dell'Unione nei seguenti 7 settori: Sistema di informazione Schengen; Sistema di informazione visti; Eurodac; Sistema di ingressi/uscite; Sistema europeo di informazione e autorizzazione ai viaggi; Sistema europeo di informazione sui casellari giudiziari riguardo ai cittadini di paesi terzi e apolidi; Interoperabilità.

Complessivamente, la Bozza di Regolamento sembra andare nella direzione di una strumentazione di c.d. *public enforcement* complementare a (e separata da) quella di c.d. *private enforcement* attinente al diverso tema della responsabilità civile per i danni causati da sistemi di IA. Quest'ultimo tema ha formato oggetto di specifica e separata considerazione da parte del Parlamento europeo in studi e progetti normativi (v. in particolare il già richiamato *Draft report* del 27 aprile 2020 della commissione giuridica del Parlamento europeo "JURI" sulla responsabilità civile, su cui la notizia [2020/2\(3\)SO](#); lo studio pubblicato dal Parlamento europeo nel luglio 2020 dal titolo "Intelligenza artificiale e responsabilità civile", su cui la notizia [2020/3\(5\)EWDM](#)) culminati nella ricordata Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)), contenente una serie di raccomandazioni e indicazioni finalizzate ad indirizzare la futura disciplina della responsabilità civile applicabile al funzionamento dei sistemi di intelligenza artificiale e una proposta di regolamento (su cui la notizia [2020/4\(1\)SG](#)).

SALVATORE ORLANDO

<https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206>

[2021/2\(2\)CR](#)

***Il comunicato del 23.04.2021 dello European Data Protection Supervisor sulla proposta dell'Artificial Intelligence Act in particolare sul riconoscimento facciale.***

Il 23 aprile 2021 il Garante europeo della protezione dei dati ("*European Data Protection Supervisor*" o "**EDPS**") ha rilasciato un comunicato stampa con cui ha commentato la proposta di regolamento europeo per l'Intelligenza Artificiale ("*Artificial Intelligence Act*") presentata dalla Commissione europea il 21 aprile 2021, su cui v. la notizia [2021/2\(1\)SO supra](#).

Wojciech Wiewiórowski, presidente dell'EDPS, si è dichiarato orgoglioso dell'iniziativa e particolarmente favorevole all'approccio "*risk-based*" su cui si fonda la proposta, in quanto questo permetterebbe di sfruttare i benefici derivanti da numerosi sistemi di intelligenza artificiale che presentano un rischio minimo per il diritto alla privacy e alla protezione dei dati personali dei cittadini.

Tuttavia, il Garante europeo ha criticato l'approccio adottato dalla Commissione con riferimento all'utilizzo dei sistemi di identificazione biometrica a distanza – compreso il riconoscimento facciale – in spazi accessibili al pubblico, considerato dall'EDPS non sufficientemente rigoroso.

La proposta di regolamento, infatti, pur ponendo in via generale un divieto di utilizzare tali sistemi, ammette alcune eccezioni quando l'utilizzo risulti strettamente necessario per il perseguimento di determinate finalità di ordine pubblico - quali la ricerca di potenziali vittime di reati (es. minori scomparsi), la prevenzione di una minaccia specifica, sostanziale e

imminente alla vita di una persona o di un attentato terroristico, l'individuazione, localizzazione, identificazione o perseguimento di una persona sospettata di aver commesso alcuni reati di particolare gravità (es. terrorismo, tratta di esseri umani, pedopornografia, truffa, falsificazione di monete, corruzione). In questi casi – sulla base della proposta di regolamento - il riconoscimento biometrico a distanza potrà essere ammesso all'esito di una specifica valutazione della gravità della situazione e delle conseguenze per i diritti e le libertà dei soggetti coinvolti, in modo proporzionato, temporalmente e geograficamente limitato, e sulla base di una preventiva autorizzazione del giudice (salvo casi di emergenza in cui l'autorizzazione potrà essere successiva). In ogni caso viene rimesso ai singoli Stati decidere se autorizzare queste forme di riconoscimento biometrico, con quali modalità e per quali reati.

Il Garante europeo già in passato aveva manifestato alla Commissione l'esigenza di assumere un atteggiamento restrittivo nei confronti dei sistemi di riconoscimento automatico in spazi accessibili al pubblico delle caratteristiche umane come i volti, l'andatura, le impronte digitali, il DNA, la voce, la digitazione e altri segnali biometrici o comportamentali. Pertanto, nel comunicato stampa in esame il presidente Wiewiórowski si è dichiarato dispiaciuto del fatto che la Commissione si sia discostata dall'indicazione del Garante di introdurre un divieto assoluto all'uso di sistemi identificazione biometrica a distanza e ha ribadito la necessità di adottare un approccio più rigoroso. Tali sistemi, infatti, con lo sviluppo dell'intelligenza artificiale potranno presentare rischi particolarmente elevati di intrusione nella vita privata dei cittadini, in violazione dei principi democratici su cui si fonda l'Unione.

Alla luce di quanto sopra, l'EDPS si è impegnato ad analizzare in maniera approfondita la proposta della Commissione al fine di rafforzare la protezione degli individui e della società nel suo complesso. In particolare, il *Supervisor*, conformemente al suo ruolo istituzionale, provvederà ad individuare i limiti per quegli strumenti che possono rappresentare un rischio per i diritti fondamentali alla privacy e alla protezione dei dati.

CHIARA RAUCCIO

[https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative\\_en](https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en)

2021/2(3)CR

### **Il parere del Garante Privacy del 25.03.2021 sul sistema di riconoscimento facciale SARI Real Time da parte del Ministero dell'Interno**

Il 25 marzo 2021 il Garante per la protezione dei dati personali (di seguito anche “Garante privacy” o “Garante”) ha espresso il proprio parere in merito all'utilizzo del sistema Sari Real Time da parte del Ministero dell'Interno. Il sistema in esame - ad oggi non in uso – consentirebbe attraverso una serie di telecamere installate in una determinata area geografica di analizzare in tempo reale i volti dei soggetti ripresi, confrontandoli con una banca dati predefinita (c.d. “*watch-list*”), che può contenere fino a 10.000 volti. Qualora, attraverso un algoritmo di riconoscimento facciale, venisse riscontrata una corrispondenza tra un volto presente nella *watch-list* ed un volto ripreso da una delle telecamere, il sistema invierebbe un *alert* agli operatori delle Forze di Polizia. Il sistema è stato progettato e sviluppato come soluzione mobile installabile direttamente presso il luogo dove si rendesse necessario al fine

di supportare – e non sostituire – le Forze di Polizia nella gestione dell'ordine e della sicurezza pubblica.

Il Garante ha espresso un parere negativo sull'utilizzo di tale sistema in quanto mancherebbe un'adeguata base giuridica su cui fondare il trattamento di dati personali (come richiesto dagli Artt. 6 e 9 del GDPR). Il sistema, infatti, comporterebbe il trattamento di enormi quantità di dati biometrici che, a seconda dei casi, potrebbero rientrare anche tra le categorie particolari di dati personali (ad esempio, dati idonei a rivelare opinioni politiche, sindacali o religiose nel caso in cui le telecamere venissero installate in occasione di manifestazioni pubbliche). Inoltre, esso non si limiterebbe ad acquisire i dati di soggetti predeterminati come i sospettati di reati, ma finirebbe per raccogliere indiscriminatamente i dati biometrici di tutte le persone presenti nello spazio monitorato. Si passerebbe così, a giudizio del Garante, da una sorveglianza mirata di alcuni individui alla possibilità di una vera e propria sorveglianza di massa.

Alla luce di ciò, la base giuridica del trattamento difficilmente potrebbe essere rinvenuta nel legittimo interesse del Viminale in quanto l'interesse a garantire la sicurezza nazionale deve essere bilanciato con i diritti e le libertà fondamentali dei soggetti interessati. L'intrusione nella vita privata degli individui coinvolti comporterebbe una sproporzionata e ingiustificata lesione del diritto fondamentale alla privacy e alla protezione dei dati. Conseguentemente, secondo il Garante privacy, un trattamento del genere deve essere necessariamente fondato su una norma di legge che lo autorizzi e lo disciplini in maniera adeguata, tenendo conto di tutti i diritti e le libertà coinvolte e definendo le situazioni e le modalità in cui è possibile l'uso di tali sistemi, senza lasciare una discrezionalità ampia a chi li utilizza. La legge, inoltre, dovrebbe definire i criteri di individuazione dei soggetti che possono essere inseriti nella *match-list* e stimare le conseguenze in caso di c.d. “falsi positivi”. Infine, il Garante segnala l'esigenza di assicurare l'accuratezza dei sistemi e di contrastare il rischio di discriminazione con particolare riguardo alle persone appartenenti a minoranze etniche, le quali potrebbero con maggiore facilità essere erroneamente identificate dagli algoritmi, posto che essi sono notoriamente basati su stime statistiche, “intrinsecamente fallibili”, di corrispondenza tra elementi confrontati.

Il Garante ha sottolineato che una norma del genere, ad oggi, non è presente nel nostro ordinamento giuridico e non può essere rinvenuta in nessuna delle fonti normative individuate dal Ministero dell'Interno in materia di pubblica sicurezza e persecuzione dei reati.

CHIARA RAUCCIO

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877>

2021/2(4)FP

**Lo studio del 05.02.2021 pubblicato dal Parlamento europeo sulla responsabilità delle piattaforme *online*.**

A febbraio 2021 è stato pubblicato lo studio sulla responsabilità delle piattaforme online (*Scientific Foresight Unit* - PE 656.318) commissionato dal *Panel for the Future of Science and Technology* al Centro di Eccellenza Jean Monnet *on the Regulation of Robotics and Artificial Intelligence* della Scuola Sant'Anna di Pisa (lo “**Studio**”). Lo Studio si colloca al centro del

dibattito sul crescente rilievo sociale ed economico assunto dalle piattaforme *online* nel corso dell'ultimo decennio. L'incremento del loro impiego nelle operazioni di scambio di beni e servizi, la pervasività nell'accesso e nella diffusione di informazioni non permettono più di ignorare il problema legato al controllo che le piattaforme possono o, in taluni casi, devono esercitare sui contenuti ospitati (*hosting*). Esperienze recenti hanno difatti dimostrato come il loro utilizzo agevoli attività illegali di varia natura e dia, di conseguenza, luogo a nuove forme di vulnerabilità: diffusione di contenuti offensivi, pirateria *online*, *bate speech* e disinformazione, violazioni delle norme sul *copyright* e sulla tutela dei minori, *data protection breach*, incitamento al terrorismo. Più intensa si è pertanto fatta l'esigenza di una risposta unitaria in termini di regolazione per definire il ruolo di prevenzione e la responsabilità che le piattaforme assumono per le attività realizzate attraverso di esse. La prima sezione dello Studio muove dalla valutazione dell'attuale contesto normativo, con particolare riferimento alla Direttiva e-commerce e alle eccezioni che essa dispone nei riguardi della responsabilità delle piattaforme. Dall'analisi compiuta ad ampio raggio sulle fonti di *hard* e di *soft law*, emergono alcune coordinate dalle quali lo Studio suggerisce di muovere per regolare questo fenomeno. Da un lato, la scelta, condivisa dagli autori dello Studio, di non adottare un approccio *one-size-fits-all*. Viene osservato come lo stesso Parlamento Europeo abbia riconosciuto, attraverso la Risoluzione del 2017 «*l'estrema difficoltà di concordare a livello di UE un'unica definizione di piattaforme online che sia giuridicamente pertinente e adeguata alle esigenze future, a causa di fattori quali la grande varietà di tipi delle piattaforme online esistenti e dei loro settori di attività nonché del mondo digitale in rapido cambiamento*» (Risoluzione del Parlamento europeo del 15 giugno 2017 sulle piattaforme online e il mercato unico digitale (2016/2276(INI)), paragrafo 6: [https://www.europarl.europa.eu/doceo/document/TA-8-2017-0272\\_IT.html](https://www.europarl.europa.eu/doceo/document/TA-8-2017-0272_IT.html)). Dall'altro lato, viene evidenziata l'esigenza di non rinunciare a definire alcune classi di riferimento all'interno delle quali inquadrare l'economia delle piattaforme. Nello Studio si nota come il quadro normativo attuale contenga un'ampia serie di definizioni specifiche per singoli segmenti di regolazione, raramente comunicanti e di difficile coordinamento fra loro. La proposta dello Studio è dunque quella di abbandonare un proposito di codificazione di una *law of platform*, adottando invece una prospettiva funzionale di classificazione *case-by-case* delle diverse strutture digitali. Questa tassonomia fa comunque riferimento ad una identificazione a monte della nozione di *online platform* come entità che «*(i) offer (primarily) OTT digital services or infrastructures to users, (ii) are or can be operated as a two- or multi-sided market business model, but may choose not to do so, and (iii) allow the overall facilitation of interaction of the different sides of the market, even when there is no direct interaction among them*» (Studio, p. 16). Su questa base, lo Studio propone una mappatura di diverse categorie di piattaforme sulla base delle attività svolte, del settore di rilevanza, delle modalità di utilizzo dei dati, degli attori coinvolti, della fonte dei proventi e del livello di controllo sui contenuti. La seconda sezione dello Studio approfondisce l'analisi della responsabilità legale delle piattaforme e formula alcune *policy options* a disposizione del Parlamento, sconsigliando un mantenimento inalterato dello *status quo*. Le proposte muovono dalla considerazione di criteri differenti (analisi costi-benefici, sostenibilità, coerenza con gli obiettivi dell'Unione, impatto etico e sociale, etc.) e dal grado progressivo di pervasività della regolazione. Il gruppo di ricerca suggerisce inoltre l'adozione di due approcci complementari: l'uno, volto a considerare la regolazione della responsabilità delle piattaforme come parte di una strategia più ampia di creazione di un ambiente digitale sicuro; l'altro, diretto a costruire un regime *technology specific*, formato da strumenti atti a porre rimedio a specifiche violazioni da parte di piattaforme con precise caratteristiche. La prima proposta consiste nella diffusione di iniziative volte al rafforzamento della consapevolezza e dell'educazione degli utenti di servizi di piattaforme *online* sulle potenzialità lesive derivanti da un loro utilizzo. Viene tuttavia osservato che questa misura, se non coordinata con altre

più incisive, rischia di risultare estremamente inefficiente, poiché la sola informazione ha una capacità di impatto del tutto marginale per gli utenti e non è dunque in grado di indirizzare le scelte verso piattaforme che mantengano *standard* più elevati di tutela. Una seconda proposta attribuisce alle autorità europee un ruolo di incentivo alla *self regulation* delle piattaforme, attraverso *voluntary commitments*. Lo Studio osserva che questi meccanismi hanno l'indubbio vantaggio di coinvolgere i grandi *players* nella definizione delle regole e nella ricerca di soluzioni condivise, ma scontano il problema del non necessario allineamento fra interessi pubblici e privati. Si nota anche che l'autoregolazione viene di frequente formulata attraverso impegni generici e con obiettivi non ben definiti, ostacolandone così l'*enforcement*. La terza proposta suggerisce dunque di stabilire un regime di co-regolazione fra soggetto pubblico e attori privati. Secondo questo modello, le autorità pubbliche svolgerebbero delle funzioni di supervisione più penetrante sul rispetto delle pratiche di autoregolazione delle piattaforme, favorendo la creazione di *sandboxes* per testare alcune soluzioni più innovative (come l'utilizzo degli algoritmi per la identificazione degli *hate speeches*). L'ultima proposta è quella che riconosce infine il ruolo più pervasivo della regolazione europea. Due sono in particolare gli obiettivi identificati nello Studio. Il primo è quello di introdurre specifici obblighi primari in capo alle piattaforme nel *design* delle proprie infrastrutture e nel monitoraggio sui contenuti. Le piattaforme sarebbero, ad esempio, obbligate ad attività di *reporting* standardizzato sulle modalità con le quali hanno svolto il monitoraggio, all'adozione di filtri automatici e sistemi di riconoscimento di contenuti inappropriati, ad obblighi di *compliance* sulla neutralità dei processi e sulla diversificazione dei servizi. Il secondo è quello di definire un regime uniforme di responsabilità, sulla base di due possibili modelli. Una prima via consisterebbe nell'adattamento della disciplina introdotta dalla Direttiva E-Commerce, per come interpretata e applicata nel corso degli anni dalla Corte di Giustizia Europea. Questa soluzione garantirebbe un grado elevato di certezza, ove accompagnata da opportuni chiarimenti, quali la distinzione fra "*specific content monitoring obligations*" e "*general duty of care*" della piattaforma. Una via ulteriore passerebbe invece dall'armonizzazione, a livello europeo, di alcune delle condizioni per ritenere la piattaforma responsabile per i contenuti e le condotte degli utenti. È il caso, ad esempio, della responsabilità per danni, ove la piattaforma sia rimasta inerte nonostante sussistessero prove evidenti di una condotta illecita perpetrata attraverso di essa, o ancora, di forme di responsabilità in specifici settori, come quello della vendita di prodotti nocivi. Questa linea di *policy*, anche in via complementare rispetto ad altre opzioni suggerite nello studio, avrebbe il merito di garantire un livello più elevato di tutela degli utenti, assicurando allo stesso tempo il *level playing field* fra gli operatori.

FEDERICO PISTELLI

[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS\\_STU\(2021\)656318\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf)

2021/2(5)FP

### **I *Final Reports* del marzo 2021 del gruppo di esperti dell'Osservatorio sulla *platform economy*.**

L'*Observatory for the Online Platform Economy*, costituito dalla Commissione Europea per studiare il fenomeno delle piattaforme digitali e per fornire una consulenza sulla *digital strategy* europea (vedi notizia [2020/3\(4\)FP](#)), ha pubblicato cinque *reports* a conclusione del suo primo

mandato. Ciascuno di essi corrisponde ad un preciso *workstream*, che il Gruppo di Esperti ha preso a riferimento per affrontare ad ampio raggio lo studio dell'economia delle piattaforme digitali: l'individuazione di parametri econometrici per misurare adeguatamente il mercato, il problema del trattamento differenziato degli utenti, l'utilizzo dei dati nell'ecosistema digitale ed il profilo del potere delle piattaforme. Quest'ultimo, in particolare, nasce con l'obiettivo di definire la posizione di potere (*power*) che contraddistingue il funzionamento dell'economia delle piattaforme digitali, rendendolo un unicum rispetto a fenomeni apparentemente analoghi di dominazione di un'impresa sul mercato. La posizione di potere che connota le piattaforme *online* non è difatti inquadrabile unicamente secondo i canoni tradizionali del *market power*, poiché il controllo viene esercitato su scala molto più ampia. Esso non si limita all'assoggettamento economico degli utenti del servizio, ma si estende sulla collettività, influenzando i comportamenti di consumatori, professionisti, individui e, in ultima analisi, della società nel suo insieme. L'emergenza da COVID-19 ha determinato un aumento esponenziale del volume di attività realizzate attraverso piattaforme *online*, dal commercio di beni sui *marketplaces*, all'ingegneria dei trasporti, fino alle iniziative legate alla cultura, all'educazione scolastica e alla tutela sanitaria. Il *report* struttura l'analisi in due sezioni, nelle quali si dà prima conto delle diverse fonti e delle tipologie di potere esercitato dalle piattaforme, per poi concludere in ordine agli aspetti che meritano particolare attenzione.

In particolare, il Gruppo di Esperti individua tre circostanze che definiscono l'unicità del potere esercitato dalle piattaforme. In primo luogo, esse assumono la posizione di *gatekeeper*, ossia di necessario *trading partner* per la collocazione di specifici prodotti sul mercato. Se, ad esempio, lo sviluppatore di un'app vuole rendere disponibile il *software* su iPhone deve interfacciarsi con la piattaforma App Store, che diviene, al tempo stesso, controparte e regolatore privato della transazione. In secondo luogo, il *business* delle piattaforme digitali si basa su strategie "darwiniane" di sopravvivenza, che richiedono l'eliminazione sistematica della concorrenza come *step* fondamentale nella crescita e nell'assunzione di una posizione di dominio sul mercato. Lo sfruttamento dell'economia di scala e del cosiddetto *network effect* si fondano difatti su di un meccanismo per cui maggiore è il numero di utenti della piattaforma, migliore è la qualità e l'ampiezza dei servizi offerti (come nel caso delle applicazioni di messaggistica o di *marketplace*). Ciò implica che il successo dei propri modelli di sviluppo dipende in gran parte da strategie di acquisizione anticipata dei concorrenti, dalla sottrazione di clientela ai *competitors* e dall'imposizione di barriere e restrizioni all'ingresso sul mercato. Questo aspetto compromette significativamente il regime di concorrenza sul mercato interno, aumentando i costi pagati dagli utenti per la migrazione verso *providers* di servizi analoghi (cd. *switching costs*), quali la perdita di crediti reputazionali o di altri benefici legati alla continuità d'uso. Consenso unanime è, però, quello attorno all'elemento ritenuto determinante nella definizione della posizione di potere delle piattaforme: il possesso e l'elaborazione di *big data*. Le piattaforme digitali hanno difatti accesso ad un'ampia porzione di dati generati dalle singole transazioni, anche di proprietà di soggetti che non ne hanno consentito direttamente la diffusione – secondo un fenomeno che viene definito in linguaggio economico *data externalities*. Il possesso di questi dati, unito alla loro elaborazione per mezzo delle tecniche di *machine learning*, consente alla piattaforma di sviluppare servizi e offrire prodotti basandosi sulla conoscenza delle preferenze degli utenti e sulla predizione dei loro bisogni futuri. Questi processi consentono pertanto di approfittare dei vantaggi dell'economia di scopo, sfruttando i medesimi fattori produttivi per la diversificazione della propria offerta. In ottica di teoria economica e regolazione, la conclusione del Gruppo di Esperti è netta: occorre ripensare ai presupposti che fino ad oggi hanno informato la disciplina normativa sulla nozione di "mercato". Essa non è più in grado di ricomprendere l'intero ambito di attività coperte dalle piattaforme digitali, non più distinguibili su base

territoriale e per comparti industriali. La soluzione proposta è quella di muovere dunque verso una nozione di “ecosistema”, da intendersi come un insieme di prodotti e servizi compatibili fra loro e in grado di esaltare le reciproche caratteristiche all’interno di un ambiente digitale (es. “*Apple ecosystem*”, “*Google ecosystem*”). L’attuale contesto normativo pare, secondo l’analisi del Gruppo di Esperti, eccessivamente incentrato sulla promozione del requisito di trasparenza, mentre minor attenzione è dedicata al contrasto a pratiche che possono risultare lesive di utenti professionisti e consumatori. In particolare, occorre chiarire il legame che sussiste fra la regolazione *ex ante* e la disciplina della concorrenza, come ambiti che non devono mirare a sovrapporsi, ma ad integrarsi fra loro. Il *report* analizza, da ultimo, il crescente ruolo assunto dalle piattaforme come intermediario fra sfera pubblica e sfera privata. Rispetto ai mass media tradizionali, le piattaforme detengono oggi il cosiddetto *opinion power*, in quanto si presentano come canali privilegiati di una comunicazione di massa fondata su di un uso dei dati e degli algoritmi in funzione di attrazione del consenso. Le piattaforme sono così in grado di definire le agende dell’azione politica, attribuendo visibilità a specifiche tematiche e figure. Gli stessi attori politici non necessitano più del filtro dei mezzi di comunicazione di massa, potendo interagire direttamente con il proprio elettorato attraverso i *social networks* e sono assistiti dagli stessi nella costruzione di campagne elettorali attraverso messaggi targettizzati a specifiche fasce di pubblico. La regolazione si è fin d’ora mossa verso l’attribuzione alle piattaforme di compiti di moderazione del dibattito, portando all’effetto paradossale per cui si riconosce - in definitiva - alle stesse il ruolo di garante della comunicazione *online*. La conclusione raggiunta dal Gruppo di Esperti è l’invito ad approfondire la comprensione di questo fenomeno, non soffermandosi unicamente sugli aspetti di carattere economico, ma analizzandoli in tutta la loro complessità. L’impatto dell’economia delle piattaforme su alcuni aspetti di rilievo centrale nelle politiche dell’Unione, come l’innovazione, la tutela della salute, la democrazia rendono questo fenomeno di prioritaria importanza all’interno dell’agenda europea.

FEDERICO PISTELLI

[https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=73962](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=73962)

2021/2(6)EP

### **Il Parere della BCE del 19.02.2021 sulla Proposta di Regolamento sui mercati di crypto-assets.**

Il 19 febbraio 2021, la Banca Centrale Europea (“**BCE**”) ha emanato un parere, ai sensi degli articoli 127, paragrafo 4, e 282, paragrafo 5, del Trattato sul Funzionamento dell’Unione Europea (TFUE), sulla proposta del 24 settembre 2020 della Commissione europea (COM(2020) 593 final-2020/0265(COD)) di un regolamento del Parlamento europeo e del Consiglio relativo ai mercati delle cripto-attività, volto a modificare la direttiva UE 2019/1937 (sulla quale v. notizia [2020/4\(2\)MS](#)).

Nonostante la BCE abbia accolto con favore l’iniziativa della Commissione europea di istituire un quadro armonizzato a livello europeo per le cripto-attività, al fine di evitare la frammentazione all’interno del mercato unico, permangono tuttavia, secondo la medesima BCE, alcuni aspetti della Proposta che necessitano di ulteriori approfondimenti e azioni correttive.

In particolare, la BCE sottolinea come, ai sensi della suddetta proposta (la “**Proposta**”), le cripto-attività (*rectius*, le due sotto-categorie dei *token* collegati ad attività e dei *token* di moneta elettronica) abbiano una evidente dimensione di sostituzione monetaria, alla luce delle tre funzioni a cui la moneta tradizionale deve assolvere: (i) mezzo di scambio, (ii) riserva di valore e (iii) unità di conto. A tal riguardo, la BCE rileva come sussista il rischio che, in considerazione dell'utilizzo concreto dei *token* collegati ad attività e dei *token* di moneta elettronica e dell'importanza sistemica che potrebbero acquisire, questi possano essere *de facto* equiparati agli strumenti di pagamento, indipendentemente dalla loro presunta funzione o applicazione principale ai sensi della Proposta. Ad avviso della BCE, al fine di prevenire il rischio di arbitraggio normativo tra i regimi applicabili ai *token* collegati ad attività e ai *token* di moneta elettronica, occorrerebbe sottoporre entrambi a requisiti analoghi e, in particolare, con riferimento ai *token* collegati ad attività, (i) imporre agli emittenti di concedere ai possessori di tali *token* diritti di rimborso sull'emittente o sulle attività di riserva, (ii) procedere alla creazione di una nuova categoria di «*token* di pagamento» volta ad assoggettare tali *token* a un insieme di requisiti identici a quelli applicabili agli emittenti di *token* di moneta elettronica e (iii) nel caso di *token* collegati ad attività significativi, ampiamente utilizzati per i pagamenti all'interno dell'Unione Europea, assoggettare gli emittenti di tali *token* significativi agli stessi requisiti di autorizzazione applicabili agli emittenti di *token* di moneta elettronica.

Inoltre, la Proposta prevede che un'autorità competente possa rifiutare l'autorizzazione a un emittente di *token* collegati ad attività, tra l'altro, qualora il modello imprenditoriale dell'emittente possa costituire una grave minaccia per la stabilità finanziaria, la trasmissione della politica monetaria o la sovranità monetaria. La BCE osserva inoltre che, qualora un dispositivo collegato ad attività fosse equiparato a un sistema o a uno schema di pagamento, la valutazione ai fini della concessione dell'autorizzazione dovrebbe rientrare nella competenza esclusiva della BCE e, a tal fine, sottolinea come il suo intervento dovrebbe tradursi nell'emissione di un parere vincolante.

In merito alla sorveglianza sui sistemi di compensazione e di pagamento, la BCE ritiene che la funzione dei dispositivi relativi ai *token* collegati ad attività e ai *token* di moneta elettronica che servono all'esecuzione di ordini di trasferimento può essere equiparata a quella di un «sistema di pagamento» qualora tale funzione presenti tutti gli elementi tipici di un sistema di pagamento, precisamente: a) un accordo formale; b) almeno tre partecipanti diretti; c) processi e procedure, secondo le regole del sistema, comuni per tutte le categorie di partecipanti; d) l'esecuzione degli ordini di trasferimento all'interno del sistema e comprendente l'avvio del regolamento e/o l'adempimento di un'obbligazione e quindi avente un effetto giuridico sugli obblighi dei partecipanti; e e) ordini di trasferimento eseguiti tra i partecipanti. All'uopo, la BCE precisa che, nella misura in cui i dispositivi relativi ai *token* collegati ad attività e ai *token* di moneta elettronica e i dispositivi che stabiliscono norme comuni per l'esecuzione delle operazioni di pagamento tra utenti finali, siano considerati «sistemi di pagamento», ad essi si applicherebbe il quadro di sorveglianza dei sistemi di pagamento dell'Eurosistema basato sui principi per le infrastrutture dei mercati finanziari emanati dal *Committee on Payment and Settlement Systems* e dall'*International Organization of Securities Commissions*.

Per quanto concerne i profili di vigilanza prudenziale, la BCE rileva come la Proposta preveda un trattamento differente tra gli emittenti di *token* di moneta elettronica significativi e gli emittenti di *token* collegati ad attività significativi. In particolare, i primi sarebbero soggetti ad un duplice sistema di vigilanza costituito dall'*European Banking Authority* (EBA) e dall'autorità nazionale competente, mentre gli altri soltanto alla vigilanza dell'EBA. Tale approccio potrebbe comportare incongruenze e duplicazioni dei compiti di vigilanza tra le

autorità coinvolte che potrebbero addirittura sfociare in misure confliggenti adottate dai regolatori coinvolti.

EUGENIO PROSPERI

<https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52021AB0004&from=IT>

2021/2(7)EP

### **Il comunicato di Consob e Banca d'Italia sui crypto-assets del 28.04.2021.**

Il 28 aprile 2021, in considerazione dell'assenza di un quadro normativo unitario in ambito europeo, la Commissione Nazionale per le Società e la Borsa (Consob) e la Banca d'Italia (le "Autorità"), congiuntamente, hanno rilasciato un comunicato stampa, mediante il quale hanno inteso rappresentare gli elevati rischi connessi con l'operatività in cripto-attività (*crypto-asset*), rivolgendosi in particolare ai piccoli risparmiatori (il "Comunicato").

Il Comunicato si è reso necessario stante il riscontrato interesse crescente della collettività, a livello europeo e internazionale, nei confronti delle cripto-attività. A tal riguardo, le Autorità hanno rilevato come, data l'assenza di un quadro regolamentare di riferimento, l'operatività in cripto-attività presenti determinati rischi che comprendono, *inter alia*, (i) la scarsa disponibilità di informazioni in merito alle modalità di determinazione dei prezzi, (ii) la volatilità delle quotazioni, (iii) l'assenza di tutele legali e contrattuali, di obblighi informativi da parte degli operatori e di specifiche forme di supervisione su tali operatori nonché di regole a salvaguardia delle somme impiegate. Inoltre, le Autorità sottolineano la presenza di rischi insiti nella tecnologia applicabile alle cripto-attività quali, ad esempio, la perdita a causa di malfunzionamenti, attacchi informatici o smarrimento delle credenziali di accesso ai portafogli elettronici.

Le Autorità hanno, inoltre, richiamato, la proposta di Regolamento UE per disciplinare l'emissione, l'offerta al pubblico, la prestazione dei servizi e il contrasto agli abusi di mercato in relazione alle diverse tipologie di cripto-attività, su cui la BCE ha rilasciato un parere in data 19 febbraio 2021 (vedi in questa la notizia [2021/2\(6\)EP](#)).

In conclusione, le Autorità dando atto della totale non soggezione delle cripto-attività ad alcuna forma di supervisione o di controllo da parte delle autorità di vigilanza, invitano la collettività a prestare particolare attenzione con riferimento a questo tipo di investimenti.

EUGENIO PROSPERI

[https://www.consob.it/web/consob/dettaglio-news/-/asset\\_publisher/hZ774IBO5XPe/content/comunicato-stampa-consob-banca-d-italia-del-28-aprile-2021/10194](https://www.consob.it/web/consob/dettaglio-news/-/asset_publisher/hZ774IBO5XPe/content/comunicato-stampa-consob-banca-d-italia-del-28-aprile-2021/10194)

2021/2(8)MG

**La sentenza 2631 del Consiglio di Stato del 29.03.2021 nel caso Facebook (gratuità del servizio e divieto di pratiche commerciali scorrette).**

La pronuncia del Consiglio di Stato, Sez. VI n. 2631 del 29 marzo 2021 conferma la sentenza del Tribunale amministrativo regionale per il Lazio, Sez. I, 10 gennaio 2020 n. 260 con la quale è stato parzialmente accolto il ricorso proposto dalla società Facebook Ireland Limited (“**FB**”) nei confronti del provvedimento dell’Autorità garante della concorrenza e del mercato n. 27432 del 29 novembre 2018 (il “**Provvedimento**”).

Con il Provvedimento, l’Autorità garante della concorrenza e del mercato (“**AGCM**”) aveva contestato a FB due distinte pratiche commerciali scorrette in violazione degli artt. 20, 21, 22, 24 e 25 d.lgs. 6 settembre 2005, n. 206 (cd. “**Codice del consumo**”):

- la “Pratica a)-pratica ingannevole” consisteva nelle “*violazione degli artt. 20, 21 e 22 del Codice del consumo*”, in quanto l’Autorità aveva rilevato che “*Sino al 15 aprile 2018, l’utente che accedeva alla homepage di FB per registrarsi sulla Piattaforma (sito web e app), a fronte di un claim sulla gratuità del servizio offerto “Iscriviti E’ gratis e lo sarà per sempre”, non trovava un altrettanto evidente e chiaro richiamo sulla raccolta e uso a fini commerciali dei propri dati da parte di FB*”;

- la “Pratica b)-pratica aggressiva” si riferiva alla “*violazione degli artt. 20, 24 e 25 del Codice del consumo, in quanto il professionista eserciterebbe un indebito condizionamento nei confronti dei consumatori registrati, i quali, in cambio dell’utilizzo di FB, verrebbero costretti a consentire a FB/terzi la raccolta e l’utilizzo, per finalità informative e/o commerciali, dei dati che li riguardano (informazioni del proprio profilo FB, quelle derivanti dall’uso di FB e dalle proprie esperienze su siti e app di terzi), in modo inconsapevole e automatico, tramite un sistema di preselezione del consenso alla cessione e utilizzo dei dati, risultando indotti a mantenere attivo il trasferimento e l’uso dei propri dati da/a terzi operatori, per evitare di subire limitazioni nell’utilizzo del servizio, conseguenti alla deselezionè*”.

Il TAR per il Lazio, con la sentenza n. 260/2020 e quella gemella n. 261/2020 emessa in pari data, aveva respinto le censure edotte da FB con riferimento alla parte del Provvedimento riferita alla “Pratica a)” (pratica ingannevole), confermando le sanzioni inflitte dall’AGCM (sul punto v. la notizia [2020/1\(4\)MG](#)); diversamente aveva accolto il ricorso proposto da FB con riferimento a quella parte del Provvedimento riferita al comportamento indicato come “Pratica b)” (pratica aggressiva).

Nei confronti della sentenza del TAR per il Lazio 260/2020 hanno proposto appello sia FB (nella parte in cui la sentenza ha respinto l’impugnazione proposta da FB, con riferimento alla Pratica a), ossia la pratica ingannevole), sia l’AGCM (nella parte in cui la sentenza ha accolto l’impugnazione proposta in primo grado da FB, con riferimento alla Pratica b), ossia la pratica aggressiva).

Il Consiglio di Stato, con riferimento all’appello proposto da FB ha affermato che – seppure si volesse aderire alla tesi della parte appellante secondo cui il dato personale sarebbe una *res extra commercium* - tale impostazione non sarebbe in ogni caso di ostacolo all’applicazione della disciplina consumeristica e neanche renderebbe esclusivamente applicabile, in quanto normativa speciale, il GDPR. Infatti, in primo luogo, il Collegio afferma che nonostante la tesi per la quale i dati personali sarebbero una *res extra commercium*, è evidente che qui essi hanno subito una “patrimonializzazione” da parte di FB. E tale patrimonializzazione avviene all’insaputa dell’utente che è persuaso di iscriversi gratuitamente alla piattaforma, mentre invece i suoi dati vengono impiegati per effettuare una profilazione a fini commerciali. In secondo luogo, secondo il Collegio, l’ambito operativo della disciplina speciale costituita dal GDPR non è assoluto e non esclude – come sostenuto da FB - l’applicazione di altre discipline, quale il Codice del Consumo, dovendosi piuttosto

ricavare dall'interpretazione dello stesso GDPR (e del suo Considerando 9 in particolare) l'«esigenza di garantire “tutele multilivello”». Conseguentemente il Consiglio di Stato ha respinto l'appello proposto da FB.

Il Consiglio di Stato, inoltre, con riferimento all'appello proposto dall'AGCM ha affermato che la “pre-attivazione” della piattaforma FB (vale a dire la “preselezione” delle opzioni a disposizione) non solo non comporta alcuna trasmissione di dati in modo diretto ed immediato dalla piattaforma FB a quella di soggetti terzi, ma è seguita da una ulteriore serie di passaggi necessitati, in cui l'utente è chiamato a decidere se e quali dei suoi dati intende condividere al fine di consentire l'integrazione tra le piattaforme. Conseguentemente, il Consiglio di Stato ha respinto anche l'appello proposto dall'AGCM.

MARISTELLA GIANNINI

<https://www.giustizia-amministrativa.it/web/guest/provvedimenti-cds>

2021/2(9)DPDM

### **La comunicazione di addebiti del 30.04.2021 della Commissione europea ad Apple per abuso di posizione dominante per le regole delle app di musica in *streaming* su App Store.**

Il 30 aprile 2021 la Commissione Europea ha pubblicato una comunicazione di addebiti (“*Statement of Objections*”) contro Apple, sostenendo che la società americana ha abusato della sua posizione dominante, ex articolo 102 TFUE, nel mercato della distribuzione di applicazioni di streaming musicale. In base alle risultanze preliminari acquisite dalla Commissione, Apple ha una posizione dominante ed è un *gatekeeper* per gli utenti di iPhone e iPad attraverso la propria piattaforma online di distribuzione di app, l'App Store, in quanto per gli sviluppatori di app, l'App Store è la sola porta di accesso ai consumatori che usano *smart mobile devices* che utilizzano il sistema operativo iOS di Apple. La Commissione ha rilevato innanzitutto la criticità delle regole che prevedono l'uso obbligatorio del meccanismo di acquisto in-app di Apple imposto agli sviluppatori di applicazioni di *streaming* musicale per la distribuzione delle loro applicazioni attraverso l'App Store. Inoltre, secondo gli addebiti, Apple imposterebbe regole (di natura contrattuale e di design informatico) rigide e più onerose nell'App Store a svantaggio dei concorrenti, con ciò privando i consumatori finali di informazioni che consentirebbero loro di operare scelte di *streaming* musicale più economiche, e, quindi, distorcendo la concorrenza.

Lo *Statement of Objections* riguarda l'applicazione di queste regole a tutte le applicazioni di *streaming* musicale che competono con la applicazione di *streaming* musicale di Apple “Apple Music” nello Spazio Economico Europeo (SEE).

La comunicazione di addebiti segue un'indagine già avviata dalla Commissione europea e una denuncia di Spotify. In particolare, il 16 giugno 2020, la Commissione europea, nella veste di regolatore europeo della concorrenza e del mercato, ha aperto un'indagine sulle condizioni dell'App Store di Apple praticate nei confronti degli sviluppatori di app di *streaming* di musica. Ciò seguiva alla denuncia sporta l'anno precedente da parte del fornitore di musica in *streaming* Spotify, concorrente di Apple Music, attraverso la quale veniva richiesto l'intervento del regolatore per ristabilire una situazione di libera concorrenza nel mercato europeo dei servizi di *streaming* musicale. A questa denuncia, in data 5 marzo 2020, si aggiungeva quella di un distributore di e-book e audiolibri, il quale sollevava le medesime

questioni in relazione all'app di distribuzione *online*, Apple Books. Veniva richiesto alla Commissione europea di valutare se le condizioni applicate da Apple nei contratti di licenza con gli sviluppatori di app, in merito alla distribuzione di queste attraverso l'App Store, e l'imposizione dell'uso del sistema proprietario di acquisti in-app di Apple (*in-app purchase*: "IAP"), limitassero in maniera anticoncorrenziale la possibilità per gli sviluppatori di informare gli utenti di iPhone e iPad delle opportunità alternative di fruizione dei medesimi servizi al di fuori della piattaforma di Apple. Questo perché gli utenti di iPhone e iPad possono scaricare applicazioni che non si trovano sul web solo attraverso l'App Store.

In dettaglio, le disposizioni esaminate dal regolatore nei contratti di licenza impongono, in primo luogo, l'uso del sistema IAP per la distribuzione di contenuti digitali a pagamento, attraverso cui Apple addebita agli sviluppatori di app una commissione del 30% su tutti gli abbonamenti venduti tramite la piattaforma. La Commissione ha verificato che la maggior parte dei fornitori di musica in *streaming* ha "trasferito" questa commissione agli utenti finali, aumentando i prezzi.

In secondo luogo, l'obbligo di usare il sistema IAP darebbe ad Apple il pieno controllo sul rapporto con i clienti dei concorrenti di Apple Music nella fornitura di *streaming* di musica, nonché la possibilità di raccogliere dati sulle attività e le offerte distribuite tramite l'App Store dai medesimi.

Inoltre, mentre Apple permette ai propri utenti di utilizzare servizi digitali in abbonamento acquistati altrove, al di fuori dell'App Store (ad esempio accedendo a contenuti di musica, e-book e audiolibri direttamente dal sito web dello sviluppatore dell'app), le sue condizioni contrattuali impediscono agli sviluppatori di app di informare gli utenti dei dispositivi Apple, iPhone e iPad, di queste possibilità alternative, che di solito sono più economiche (c.d. "*anti-steering provisions*").

Gli addebiti sono basati su risultanze e convincimenti preliminari, come allo stato acquisiti e formati dalla Commissione europea. L'invio di una comunicazione degli addebiti consente ad Apple di presentare le proprie osservazioni e difese dinanzi alla Commissione e non condiziona l'esito delle successive indagini e di un eventuale successivo contenzioso.

DOMENICO PIERS DE MARTINO

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2061?fbclid=IwAR3j2jP92hYsaCQpdVGC20nTcolJUgbcix0l20eFHeZvCKG-Prtr3b10Srk](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2061?fbclid=IwAR3j2jP92hYsaCQpdVGC20nTcolJUgbcix0l20eFHeZvCKG-Prtr3b10Srk)

2021/2(10)EMI

***Fair use e open source: la decisione della Corte Suprema degli Stati Uniti d'America del 05.04.2021 nel caso della API di Java (Oracle c/ Google).***

Il 5 aprile 2021 la Corte Suprema americana ha deciso l'annosa controversia *Google Llc v. Oracle America, Inc.*, che ha avuto inizio più di 10 anni fa dinanzi alla Corte distrettuale di San Francisco.

La questione giuridica ha seguito il processo di creazione del sistema operativo Android di Google. Infatti, durante la fase genetica del nuovo sistema operativo, Google ha utilizzato oltre 11 mila linee di codice scritto in Java, contenente varie API («*Application Programming Interface*»), al fine di velocizzare il processo di implementazione e sviluppo delle applicazioni. I codici erano stati inizialmente generati dalla società Sun Microsystem, acquistata nel 2009 da Oracle che è diventata titolare di tutti i diritti d'autore sulla piattaforma Java.

Dopo il primo grado di giudizio dinanzi alla Corte distrettuale di San Francisco che aveva respinto le istanze di Oracle, nel 2018 la Corte d'Appello ha accolto la richiesta di risarcimento, considerando l'utilizzo delle linee di codice un uso illegittimo in violazione del diritto d'autore spettante a Oracle.

Google ha, quindi, formulato un c.d. «*writ of certiorari*», rimettendo la controversia dinanzi alla Corte Suprema per la sua decisione. La richiesta di Google ha proposto due questioni. La prima, se le API di Java sono «*copyrightable*». La seconda, se l'uso da parte di Google è stato un «*fair use*». La Corte ha deciso di rispondere soltanto alla seconda domanda, in quanto in ogni caso risolutiva ove anche dovesse assumersi una risposta affermativa alla prima (e più impegnativa) questione, alla quale pertanto la Corte non ha risposto, ma la cui risposta affermativa ha presupposto per pura ipotesi al fine di affrontare la seconda questione. Interessante come la Corte, per motivare questa scelta, abbia fatto riferimento al contesto tecnologico, economico ed imprenditoriale in rapido cambiamento: «*Given the rapidly changing technological, economic, and business-related circumstances, we believe we should not answer more than is necessary to resolve the parties' dispute. We shall assume, but purely for argument's sake, that the entire Sun Java API falls within the definition of that which can be copyrighted. We shall ask instead whether Google's use of part of that API was a "fair use"*».

Il tema principale della questione e delle argomentazioni della Corte ha quindi ruotato intorno alla possibilità di considerare l'utilizzo del codice Java compiuto da Google senza la preventiva autorizzazione di Oracle, come una ipotesi di «*fair use*» e, quindi, di uso legittimo di un'opera tutelata (in ipotesi) dal *copyright*.

Il problema consequenziale attiene ai sistemi c.d. «*open source*» (come quello utilizzato da Google con Android) e alla possibilità di applicare le ipotesi derogatorie a favore di questi progetti anche nel caso di colossi del mercato digitale che, grazie a simili strutture operative, riescono ad ottenere notevoli profitti, come, d'altronde, sostenuto da Oracle dinanzi alla Corte.

Bisogna notare che le linee Java “copiate” costituiscono soltanto una piccolissima parte dell'intero codice di programmazione di Android e che, come riportato dalla Corte Suprema, le API «*allow[s] programmers to use ... prewritten code to build certain functions into their own programs*», rappresentando, di fatto, un tassello essenziale nello sviluppo della programmazione informatica.

La Corte Suprema, con parere favorevole di sei degli otto giudici, si è espressa a favore di Google, rigettando le richieste risarcitorie di Oracle. La Corte, infatti, ritiene che, sebbene l'uso delle linee di codice Java sia avvenuto senza autorizzazione da parte del titolare dei diritti d'autore, la questione proposta vada a configurare una ipotesi di «*fair use*».

Il principio («*an equitable rule of reason*») è, difatti, volto a mitigare proprio i diritti di esclusiva del titolare del *copyright* e trova riconoscimento all'interno del *Copyright Act* statunitense. Come ribadito dalla Corte nelle sue ricostruzioni, la §107 definisce il perimetro entro cui collocare le ipotesi di uso legittimo di un'opera tutelata dal diritto d'autore. In particolare, nel giudizio di bilanciamento da compiersi è richiesto che l'utilizzo sia trasformativo, ovvero che aggiunga all'opera originaria elementi e scopi nuovi, e che vadano tenuti in considerazione la quantità dell'opera protetta impiegata, lo scopo dell'attività alla base dell'uso del materiale protetto e l'impatto economico sul titolare dell'opera protetta e sull'utilizzatore della stessa.

Sul punto, la Corte sottolinea che l'utilizzo di codici Java è considerabile come un uso corretto in quanto si inserisce in una attività trasformativa avvenuta in un contesto – quello dei dispositivi mobili – e con modalità del tutto differenti rispetto all'utilizzo originario ed in quanto esso è finalizzato a facilitare le operazioni di programmazione che già sfruttavano le linee dei codici in questione.

La sentenza, invece, come detto, non si esprime in maniera definitiva sulla controversa tutela da offrire ai titolari di *copyright* sui codici di programmazione e sulla possibilità di prevedere una forma di equo compenso nel caso di usi che abbiano generato notevoli vantaggi economici per l'utilizzatore, come nel caso di specie e come evidenziato dal giudice Thomas nella sua *dissenting opinion*.

È indubbio che la portata di questa sentenza possa generare prospettive nuove sia nell'ambito dei sistemi c.d. *open source* sia nel contesto dell'applicazione del principio di *fair use* all'interno dell'ordinamento statunitense, specialmente in relazione ad attività connesse al mercato digitale.

ENZO MARIA INCUTTI

[https://www.supremecourt.gov/opinions/20pdf/18-956\\_d18f.pdf](https://www.supremecourt.gov/opinions/20pdf/18-956_d18f.pdf)

2021/3(1)DI

### **La Carta dei diritti digitali presentata dal Governo spagnolo il 14 luglio 2021.**

Il 14 luglio 2021 il governo spagnolo ha presentato la *Carta derechos digitales* (“**Carta**”), un documento non normativo che afferma il valore della persona e della dignità umana nella definizione delle regole e delle politiche della nuova realtà digitale. Redatto da un gruppo di esperti di discipline diverse, la *Carta* è il risultato di circa un anno di lavori e di due consultazioni pubbliche. Il testo si compone di ventotto disposizioni suddivise in sei sezioni e anticipate da un preambolo che da conto delle ragioni dell'intervento, centrale nella c.d. *Plan España Digital 2025*.

La prima sezione della *Carta*, intitolata *Derechos de libertad*, si apre con il riferimento al rispetto negli ambienti digitali dei diritti fondamentali riconosciuti nelle diverse carte e dichiarazioni e prosegue con l'affermazione del diritto all'identità, alla protezione dei dati (con esplicito richiamo al Regolamento UE 2016/679, il GDPR) e al diritto all'utilizzo di uno pseudonimo. A tal proposito, la *Carta* prevede che tale pretesa possa essere limitata solo quando l'identificazione personale sia necessaria e che sia comunque possibile l'identificazione dell'utente ove richiesto dall'autorità giudiziaria. La medesima sezione prevede poi che il ricorso a sistemi di analisi che impieghino decisioni automatizzate o la profilazione degli individui sia possibile solo quando ammesso dalla normativa nonché il diritto di tutte le persone a strumenti di sicurezza adeguati a un trattamento dei dati sicuro. La sezione si chiude demandando la disciplina della “eredità digitale” al legislatore.

La sezione successiva, dal titolo di *Derechos de igualdad*, contiene cinque articoli. Oltre al diritto alla non discriminazione, al diritto all'accesso e al contrasto al divario digitale, la sezione prevede una ricca disposizione in merito alla protezione dei minori. Tale disciplina (art. X) si apre ponendo a carico dei soggetti responsabili (es. i genitori) il compito di assicurare un uso responsabile degli ambienti digitali per garantire il corretto sviluppo del minore. Tra le altre cose, l'articolo X prevede l'introduzione di procedure per la verifica dell'età, il diritto di ricevere una formazione e un'informazione adeguate alle capacità del minore e un generale divieto di trattamento dei dati personali dei minori a fini di profilazione.

La terza sezione della *Carta* contiene disposizioni in tema di partecipazione e di informazione tramite ambienti digitali. Essa si apre con il riferimento alla neutralità della rete Internet e prosegue poi affrontando il tema dell'informazione in ambiente digitale. In particolare, l'art. XV afferma il diritto a ricevere informazioni veritiere e conformi ai

protocolli sulla trasparenza (in base ai quali comunicare se l'informazione è stata elaborata mediante processi automatizzati o se ha carattere pubblicitario o meno). La sezione in parola si conclude con tre articoli che affermano il diritto dei cittadini alla partecipazione politica per mezzi digitali, a ricevere un'educazione digitale e ad avere rapporti digitali con la pubblica amministrazione.

La quarta e la quinta sezione affrontano precise tematiche degli ambienti digitali. In una, si offrono indicazioni relative al rispetto dei diritti fondamentali dei lavoratori (art. XIX) e alla libertà di impresa in un contesto concorrenziale (art. XX) e nell'altra si prevedono disposizioni in materia di ricerca scientifica, diritto alla salute e diritto all'attività artistica-culturale, nonché in relazione all'impiego di programmi di intelligenza artificiale e di neurotecnologie. In tale quinta sezione, rubricata *Derechos digitales en entornos e específicos*, la *Carta* fa riferimento anche alla necessità dello sviluppo tecnologico di rispettare la sostenibilità ambientale e le generazioni future. La *Carta* si conclude con una sesta sezione, *Garantias y eficacia*, che riconosce la tutela dei diritti fondamentali anche in ambiente digitale.

Di tutta evidenza, la *Carta* si inserisce in una lunga lista di testi simili, adottati da altre autorità al fine di governare gli ambienti digitali affermando il rispetto dei diritti fondamentali. In tal senso, il testo spagnolo ricorda la *Dichiarazione dei diritti in Internet*, approvata dalla Camera dei Deputati nel 2015 e che conteneva già diverse disposizioni analoghe a quelle ora affermate nella *Carta* (e.g. neutralità della rete, inviolabilità dei sistemi informatici, protezione dell'anonimato).

DANIELE IMBRUGLIA

[https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta\\_Derechos\\_Digitales\\_RedEs.pdf](https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf)

2021/3(2)SO-CS

**La Corte di Cassazione subordina la validità del consenso al trattamento dei dati personali alla trasparenza dell'algoritmo che governa il servizio per il quale il consenso è prestato (ordinanza 14381 del 25 maggio 2021 a proposito di un servizio di calcolo del c.d rating reputazionale)**

Con l'ordinanza n. 14381/2021, la sezione I della Corte di Cassazione si è pronunciata sui requisiti di validità del consenso al trattamento dei dati personali degli aderenti a una piattaforma web volta ad elaborare i loro profili reputazionali attraverso un calcolo algoritmico (l'"**Ordinanza**"). Benché l'Ordinanza riguardi una vicenda antecedente alla entrata in vigore del Regolamento UE 2016/1679 ("**GDPR**"), essa presenta sicura rilevanza in materia per il principio in essa espresso che condiziona la validità della prestazione del consenso al trattamento dei dati personali alla conoscibilità dell'algoritmo che fa funzionare il servizio per il quale il consenso è prestato.

La vicenda trae origine dal provvedimento n. 488 del 24 novembre 2016 del Garante per la protezione dei dati personali ("**Garante Privacy**") con il quale era stata vietata qualunque operazione di trattamento dei dati personali effettuata dalla piattaforma web in questione, la piattaforma "MEVALUATE" (con connesso archivio informatico) preordinata all'elaborazione di profili reputazionali concernenti persone fisiche e giuridiche. Attraverso tale piattaforma, l'associazione titolare del trattamento intendeva offrire un servizio idoneo a contrastare fenomeni basati sulla creazione di profili artefatti o inventieri, affidando a un

meccanismo di calcolo algoritmico la determinazione del c.d. “*rating* reputazionale” dei soggetti censiti. Obiettivo ultimo, pertanto, era quello di consentire a terzi interessati di poter verificare la reale credibilità di quei profili.

L'associazione Mevaluate Onlus si rivolgeva quindi al Tribunale di Roma chiedendo l'annullamento del provvedimento del Garante Privacy. Il ricorso trovava accoglimento quasi integrale da parte del Tribunale di Roma che con sentenza n. 5715/2018 del 4 aprile 2018 faceva salva l'efficacia del divieto solo in relazione al trattamento dei dati personali riguardanti soggetti terzi non associati a Mevaluate Onlus.

La decisione del Tribunale veniva infine impugnata in Cassazione dal Garante.

Ai presenti fini, ciò che più interessa evidenziare è il fatto che la Corte di Cassazione si è allontanata dai temi maggiormente disputati (con esiti opposti) davanti al Garante e al Giudice di merito, ritenendo rilevante quello dei presupposti di validità del consenso al trattamento dei dati personali. Nel complesso motivazionale che aveva permesso al Tribunale di Roma di accogliere (pressoché integralmente) il ricorso contro il provvedimento del Garante, assumeva rilievo fondamentale la riflessione sull'attività oggetto del servizio “MEVALUATE”. Il Tribunale di Roma osservava che non può negarsi all'autonomia privata la facoltà di organizzare sistemi di accreditamento di soggetti fornendo servizi “valutativi” per la conclusione di contratti e per la gestione di rapporti economici, a ciò non ostando – contrariamente da quanto ritenuto dal Garante a motivazione del suo provvedimento di divieto – neppure il difetto di una cornice normativa *ad hoc* in tema di *rating* reputazionale, stante la diffusione, nella realtà attuale, di fenomeni di valutazione e di certificazione da parte di privati a fini di attestazione di qualità e/o conformità a norme tecniche. Tanto premesso ed argomentato, il Tribunale di Roma considerava legittimo il trattamento dei dati personali dei soggetti aderenti al sistema “MEVALUATE”, in quanto, nella specie, ritenuto validato dal loro consenso.

La Corte di Cassazione, nell'Ordinanza qui in commento, ha invece sottoposto ad analisi specifica i presupposti per la validità del consenso al trattamento dei dati personali.

A tal riguardo, la norma presa in considerazione dall'Ordinanza è l'art 23 d.lgs. n. 196/2003 (“**Codice Privacy**”) nella versione antecedente all'entrata in vigore del GDPR (cfr. Cass., n. 16358/2018; Cass., n. 17278/2018). All'uopo, la Corte di Cassazione ricorda innanzitutto nell'Ordinanza in termini generali che occorre che il consenso non solo sia espresso dall'interessato in modo libero e con riguardo a uno specifico trattamento, ma, soprattutto, è necessario che l'oggetto della manifestazione di volontà sia un trattamento “chiaramente individuato” e documentato per iscritto. In particolare, la Corte evidenzia nell'Ordinanza lo stretto legame tra la manifestazione del consenso e il ruolo della informazione, e che un trattamento chiaramente individuato, per dirsi tale, presuppone che, a monte, il titolare del trattamento abbia provveduto a fornire le informazioni necessarie, ai sensi dell'art. 13 del Codice Privacy, individuandone gli elementi essenziali, gravando sul titolare l'onere di provare che il trattamento si fonda su un consenso idoneo e validamente ottenuto.

Ciò premesso, la Cassazione ha applicato i suddetti principi enunciati al caso di specie, reputando che – avuto riguardo alle caratteristiche tecnologiche del servizio (che si avvale di algoritmi di calcolo del *rating* reputazionale) e alla loro conoscibilità da parte degli interessati – la manifestazione del consenso prestata dagli aderenti alla piattaforma *de qua* non sia sufficiente a garantire la liceità del trattamento. Ciò in quanto, secondo la Cassazione, detto consenso si fonda su informazioni opache rispetto all'algoritmo impiegato dalla piattaforma per il calcolo del *rating*. Tale aspetto costituisce un passaggio cruciale della decisione. A riguardo, la Corte precisa che la scarsa trasparenza dell'algoritmo impiegato non incide solo sul “*momento valutativo del procedimento*”, bensì sulla stessa liceità del trattamento, in quanto

fondato su una base giuridica viziata. Sotto questo profilo, i giudici di legittimità contestano la decisione del tribunale di Roma, secondo il quale, i dubbi relativi al sistema automatizzato di calcolo del rating reputazionale non sarebbero decisivi, in quanto spetterebbe al mercato «stabilire l'efficacia e la bontà del risultato ovvero del servizio prestato dalla piattaforma». Questo passaggio viene particolarmente criticato dai Giudici nomofilattici, in quanto, nella loro interpretazione, esso non coglie il cuore del problema, rappresentato dal consenso prestato dagli aderenti alla piattaforma. Secondo la Corte di Cassazione, invero, «non può logicamente affermarsi che l'adesione a una piattaforma da parte dei consociati comprenda anche l'accettazione di un sistema automatizzato, che si avvale di un algoritmo, per la valutazione oggettiva di dati personali, laddove non siano resi conoscibili lo schema esecutivo in cui l'algoritmo si esprime e gli elementi all'uopo considerati». Tanto significa che la Corte ammette, in generale, la possibilità di sviluppare servizi di “rating reputazionale” basati su consenso dell'interessato, ma se l'algoritmo e gli elementi di cui si compone restano ignoti o non sono conoscibili da parte degli interessati, il requisito della consapevolezza non può dirsi soddisfatto.

In questa prospettiva, la sentenza di merito veniva dunque cassata e rinviata al medesimo Tribunale di Roma, in diversa composizione, per un nuovo esame da condursi osservando il seguente principio di diritto: «In tema di trattamento di dati personali, il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento a un trattamento chiaramente individuato; ne segue che nel caso di una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali di singole persone fisiche o giuridiche, incentrata su un sistema di calcolo con alla base un algoritmo finalizzato a stabilire i punteggi di affidabilità, il requisito di consapevolezza non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati».

SALVATORE ORLANDO / CHIARA SARTORIS

<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5796783>

[https://web.uniroma1.it/deap/sites/default/files/allegati/CASO\\_MEVALUATE\\_02.pdf](https://web.uniroma1.it/deap/sites/default/files/allegati/CASO_MEVALUATE_02.pdf)

[https://web.uniroma1.it/deap/sites/default/files/allegati/CASO\\_MEVALUATE\\_03.pdf](https://web.uniroma1.it/deap/sites/default/files/allegati/CASO_MEVALUATE_03.pdf)

2021/3(3)CR

### **Il pronunciamento congiunto EDPS - EDPB del 21 giugno 2021 sulla proposta di disciplina sul riconoscimento facciale contenuta nell'Artificial Intelligence Act**

Il 21 giugno 2021 l'EDPB (*European Data Protection Board*) e l'EDPS (*European Data Protection Supervisory*) hanno adottato un'opinione congiunta sulla proposta di regolamento europeo per l'Intelligenza Artificiale (“*Artificial Intelligence Act*” o “**AIA**”) presentata dalla Commissione europea il 21 aprile 2021 (su cui v. la notizia [2021/2\(1\)SO](#)). Pur accogliendo positivamente l'iniziativa della Commissione di regolamentare l'utilizzo dell'intelligenza artificiale nell'ambito dell'UE e l'adozione di un approccio basato sul rischio (*risk-based*), le due Autorità hanno evidenziato alcune criticità in merito alla proposta.

Innanzitutto, l'EDPS e l'EDPB sottolineano la necessità di specificare chiaramente che tutti i trattamenti di dati personali effettuati attraverso sistemi di intelligenza artificiale rientrano nell'ambito di applicabilità – oltre che dell'AIA – della normativa europea in materia di protezione dei dati. Ne consegue che un sistema di IA che implica un trattamento di dati personali, pur rispettando le condizioni previste dalla medesima proposta di

regolamento, non può considerarsi lecito e non può essere introdotto nel mercato europeo se non risulta conforme alla normativa sulla protezione dei dati personali. Inoltre, il concetto di “rischio per i diritti fondamentali” deve essere allineato a quello utilizzato nel GDPR al fine di assicurare un quadro normativo europeo coerente ed armonizzato.

L'EDPS e l'EDPB si sono poi focalizzati sull'utilizzo di sistemi di IA per la rilevazione, il riconoscimento e l'analisi dei dati biometrici. In particolare, in linea con quanto già espresso dall'EDPS in un comunicato stampa del 23 aprile 2021 (su cui v. la notizia [2021/2\(2\)CR](#)), le Autorità hanno chiesto l'introduzione di un divieto totale all'uso dell'IA per l'identificazione biometrica a distanza in spazi pubblicamente accessibili attraverso il riconoscimento automatico di caratteri biometrici o comportamentali come il volto, la voce, l'andatura, il modo di scrivere su una tastiera, le impronte digitali e il DNA, che farebbe venire meno ogni forma di anonimato in questi spazi. Allo stesso modo, il divieto dovrebbe riguardare l'utilizzo dell'IA per la creazione, attraverso l'analisi dei dati biometrici, di *cluster* in cui gli individui sono raggruppati sulla base di caratteristiche potenzialmente discriminatorie come l'etnia, il genere, l'orientamento politico e sessuale o sulla base di qualsiasi altro fattore di discriminazione vietato ai sensi dell'art. 21 della Carta dei diritti fondamentali dell'Unione Europea. Infine, l'uso di sistemi di IA dovrebbe essere vietato per la rilevazione delle emozioni delle persone fisiche (salvo casi particolari in cui tale utilizzo può avere effetti positivi sugli individui, ad esempio in ambito sanitario) e per l'assegnazione di qualsiasi tipo di *social scoring*. In particolare, i Presidenti delle due Autorità (Andrea Jelinek per l'EDPB e Wojciech Wiewiórowski per l'EDPS) hanno segnalato che tali utilizzi dell'IA andrebbero a minare nelle loro fondamenta i diritti e le libertà fondamentali riconosciuti e tutelati dall'UE (come il diritto alla libertà personale e il divieto di discriminazioni), e per questo si rende necessario un approccio precauzionale attraverso l'introduzione di un divieto generale al fine di garantire uno sviluppo dell'IA e un sistema normativo che pongano al centro l'essere umano (*human-centric*).

Gli ultimi punti affrontati nell'*opinion* riguardano il quadro istituzionale, a partire dalla previsione della proposta di AIA per la quale, nei casi in cui le istituzioni, le agenzie e gli organismi dell'Unione Europea rientrano nell'ambito di applicazione dell'AIA, l'EDPS agirebbe in qualità di autorità di vigilanza del mercato. Le Autorità richiedono che la proposta specifichi in maniera più dettagliata la portata del ruolo e dei compiti assegnati all'EDPS in qualità di autorità di vigilanza del mercato. In secondo luogo, richiedono che le autorità di controllo nazionali per la protezione dei dati siano designate quali autorità nazionali di controllo ai sensi dell'Art. 59 della proposta di AIA. Tali autorità, infatti, occupandosi già di tutelare i diritti fondamentali e di vigilare sul rispetto del GDPR e della Direttiva UE 2016/680 c.d. Law Enforcement Directive (“LED”) per i trattamenti di dati personali che coinvolgono sistemi di IA, potrebbero assicurare che l'interpretazione e l'applicazione dell'emanando regolamento sull'IA sia omogenea in tutti gli Stati Membri e sia coerente con la normativa sulla protezione dei dati personali. Infine, le Autorità hanno criticato il ruolo dominante che la proposta di regolamento prevede di attribuire alla Commissione europea nell'istituendo *European Artificial Intelligence Board* (EAIB) sostenendo che tale ultimo organo, per svolgere adeguatamente le proprie funzioni, dovrebbe essere indipendente dal potere politico e godere di una maggiore autonomia di iniziativa.

CHIARA RAUCCIO

[https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible\\_en](https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en)

2021/3(4)CM

### **Le regole sul riconoscimento facciale per le società private emesse dalla Suprema Corte del Popolo della Repubblica Popolare Cinese il 28 luglio 2021.**

Il 28 luglio 2021, la Suprema Corte del Popolo della Repubblica Popolare Cinese ha pubblicato il *Provvedimento della Corte Suprema del Popolo su diverse questioni relative all'applicazione della legge nei procedimenti civili relativi all'uso della tecnologia di riconoscimento facciale per il trattamento delle informazioni personali* (最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定, in seguito il 'Provvedimento'). Il documento costituisce, dal punto di vista del sistema delle fonti cinese, un'interpretazione giudiziale autentica, a cui è riconosciuto valore di legge e con cui la Suprema Corte è solita fissare norme e principi per la corretta applicazione delle leggi. In particolare, il Provvedimento di cui al presente commento, è composto da 16 articoli ed è pubblicato, si legge, allo scopo di 'implementare lo stato di diritto di Xi Jinping, porre al centro del sistema la persona, salvaguardare i diritti della personalità delle persone fisiche e proteggere la sicurezza dei volti dei cittadini'. Con esso la Corte Suprema 'si fa carico dei principi contenuti nel nuovo codice civile, allo stesso tempo rafforza la tutela giudiziale delle informazioni personali (fra i quali, ovviamente, il volto non può che essere sussunto nella categoria) e promuove lo sviluppo sano dell'economia digitale'. La pubblicazione ha notevole rilievo, oltre che per la sua incidenza nomofilattica, anche per la sua sostanziale portata innovativa. Esso mira a rafforzare la tutela giuridica delle informazioni sensibili, vale a dire, quelle informazioni personali che, ai sensi dei *National Standard of Information Security Technology – Personal Information Security Specification* (信息安全技术 个人信息安全规范), sono da considerarsi come potenzialmente dannose per la sicurezza degli individui e quindi oggetto di tutela rafforzata da parte dell'ordinamento. Tra le informazioni sensibili rientrano appunto le informazioni 'biometriche', vale a dire i tratti fisiognomici delle persone fisiche e che, quindi, sono oggetto di tutela rafforzata. Ma vediamo come impatta, a livello prescrittivo, il Provvedimento. Esso prevede alcune fattispecie illecite, che violano la legge sulla protezione delle informazioni personali. Esse sono: l'utilizzo di tecnologie di riconoscimento facciale per la verifica, il riconoscimento o l'analisi del volto in aree pubbliche (ad esempio, hotel, centri commerciali, banche, stazioni, aeroporti, stadi, etc.), in contrasto con disposizioni di legge; mancata comunicazione delle regole per il trattamento dei dati personali o mancata esplicitazione delle finalità, modalità o perimetro del trattamento; mancato ottenimento del consenso dell'interessato; trattamento di informazioni biometriche in difformità dal consenso ricevuto; mancata adozione delle misure di sicurezza obbligatorie per legge; fornitura di informazioni biometriche a terzi; utilizzo delle informazioni biometriche in violazione dell'ordine pubblico; trattamento delle informazioni biometriche in violazione dei principi di legalità, legittimità e necessità. Un'ulteriore novità è costituita dal fatto che per il trattamento delle informazioni biometriche sarà necessario richiedere, da parte del titolare del trattamento, ed ottenere, da parte del soggetto le cui informazioni sono raccolte, un consenso 'specifico' per questo tipo di informazioni. Il Provvedimento ha iniziato a dispiegare i suoi effetti a partire dal 1° agosto 2021.

CORRADO MORICONI

<http://www.court.gov.cn/fabu-xiangqing-315851.html>

2021/3(5)LV

### **Le Linee Guida EDPB del 7 luglio 2021 sugli assistenti vocali virtuali.**

Il 7 luglio 2021 il Comitato europeo per la protezione dei dati personali, *European Data Protection Board* (l'“**EDPB**”), ha adottato la versione definitiva, successiva a pubblica consultazione, delle Linee Guida sugli assistenti vocali virtuali - *Guidelines on virtual voice assistants* (le “**Linee Guida**”).

L'assistente vocale virtuale (*Virtual Voice Assistant*: “**VVA**”) è un programma che interpreta il linguaggio naturale tramite algoritmi di intelligenza artificiale capace di interloquire con gli esseri umani allo scopo di soddisfare le relative richieste o di compiere determinate azioni. Così, un VVA è in grado di effettuare ricerche di informazioni, di perfezionare acquisti *online*, di far ascoltare brani musicali, ma anche, nel contesto domestico - che rappresenta terreno privilegiato di applicazione di simili soluzioni - di regolare la temperatura o l'illuminazione dell'ambiente, di attivare elettrodomestici o allarmi ecc. I VVA trovano il loro supporto fisico in un dispositivo terminale dotato di microfoni e altoparlanti: un *computer*, uno *smartphone*, una *smart tv*, un *tablet* o un *device* autonomo come lo *smart speaker*.

L'EDPB, nella consapevolezza della notevole diffusione che negli ultimi anni i VVA hanno vissuto, all'interno di uno scenario ormai connotato da un avvento massiccio del digitale, raccomanda l'adozione di soluzioni conformi alla normativa europea vigente in materia di trattamento dei dati personali e di comunicazioni elettroniche.

In effetti, le Linee Guida affrontano in maniera assai definita una pluralità di aspetti relativi ai dispositivi in questione, dei quali viene delineata una definizione ed una rappresentazione dettagliata che descrive i meccanismi tecnologici sottostanti al loro funzionamento. Soprattutto, vengono evidenziati i rischi che ne derivano per gli utenti e le sfide che si profilano su un piano di *compliance* normativa.

Le Linee Guida pongono bene in luce fin da subito come sia intrinseco al funzionamento dei VVA l'accesso ad un'enorme quantità di dati personali, ivi inclusi tutti i comandi vocali degli utenti, ed al contempo come tali dati subiscano trasferimenti ai *server* remoti dei VVA stessi, con conseguente necessità di tenere in considerazione, per gli operatori che forniscono servizi di VVA, sia il Regolamento 2016/679 UE (il “**GDPR**”) che la Direttiva 2002/58 CE (la “**direttiva e-Privacy**”): viene così delineata la cornice normativa di riferimento.

Con specifico riguardo alla direttiva e-Privacy, le Linee Guida ricordano che poiché i VVA operano sempre attraverso uno dei suddetti dispositivi fisici (*smartphone*, *tablet*, *smart speaker* ecc.), essi utilizzano reti di comunicazione elettronica per accedere a questi *device*, che costituiscono “apparecchiature terminali” nel senso della direttiva e-Privacy. Di conseguenza, le disposizioni dell'art. 5, par. 3 della direttiva e-Privacy si applicano ogni volta che il VVA memorizza o accede ad informazioni nel dispositivo fisico ad esso collegato. In base a tale previsione, l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso ad informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente deve essere consentito unicamente a condizione che l'interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento, e che gli sia offerta la possibilità di rifiutare tale trattamento.

Qualsiasi operazione di trattamento di dati personali conseguente, compreso il trattamento dei dati personali ottenuti accedendo alle informazioni nell'apparecchiatura terminale, deve inoltre avere una base giuridica ai sensi dell'art. 6 GDPR per essere lecita. Poiché il titolare del trattamento, quando richiede il consenso per la conservazione o l'accesso

alle informazioni ai sensi dell'art. 5, par. 3, direttiva e-Privacy, dovrà informare l'interessato su tutte le finalità del trattamento, il consenso sarà generalmente la base giuridica più adeguata a coprire il trattamento conseguente dei dati personali. Quindi il consenso costituirà probabilmente, secondo le Linee Guida, la base giuridica sia per la memorizzazione e l'ottenimento dell'accesso a informazioni già memorizzate, che per il trattamento dei dati personali successivo a tali operazioni.

Inoltre, l'EDPB ricorda che, nell'individuazione della base giuridica appropriata, è obbligo dei titolari del trattamento tenere in ogni caso conto dell'impatto che si possa produrre sui diritti degli interessati e che l'art. 6 GDPR non può essere invocato dai *data controller* al fine di ridurre la protezione aggiuntiva fornita dall'art. 5, par. 3 direttiva e-Privacy. Quest'ultima, d'altronde, costituisce una *lex specialis* destinata a prevalere sul GDPR (come già stabilito nel Parere dello stesso EDPB 5/2019 sull'interazione tra la direttiva e-Privacy e il GDPR, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati).

Altro profilo a cui le Linee Guida dedicano attenzione riguarda l'eventualità che gli VVA registrino accidentalmente l'audio di soggetti terzi che non avevano intenzione di utilizzare i relativi servizi. Dal momento che appare altamente improbabile che un'attivazione accidentale possa essere interpretata come un consenso valido dell'interessato, i dati così raccolti dovrebbero essere cancellati.

Le Linee Guida tengono ulteriormente in considerazione le complicità che derivano dalla presenza, sullo scenario determinato dall'operatività di un VVA, di una pluralità e una concatenazione di "attori" ('fornitore', 'progettista', 'sviluppatore', 'integratore', 'proprietario', 'utente', come definiti, rispettivamente, nelle Linee Guida) il che rende difficoltosa l'individuazione dei soggetti del trattamento dei dati personali e la conseguente ripartizione di obblighi e responsabilità, nonché l'identificabilità, da parte dell'interessato, dei soggetti coinvolti al fine del corretto esercizio dei suoi diritti. Pur in tale scenario complesso, secondo le Linee Guida si può comunque prospettare a carico del fornitore dei servizi VVA almeno l'obbligo di rilasciare idonea informativa conforme al GDPR non solo agli utenti registrati ai servizi VVA, ma anche a chi non è registrato e possibilmente persino agli utenti c.d. accidentali.

Quanto alla *data retention*, l'EDPB ricorda che in conformità al principio di limitazione della conservazione dei dati di cui al GDPR, i VVA dovrebbero conservare i dati per un tempo non superiore a quello necessario per le finalità per le quali i dati personali sono trattati. Pertanto, i periodi di conservazione dei dati dovrebbero essere legati alle diverse finalità di trattamento.

Ancora, l'EDPB fa notare come fra i dati personali trattati dai VVA vi siano dati rientranti nelle categorie particolari *ex art. 9 GDPR*. In particolare, in questo contesto le Linee Guida osservano che gli stessi dati vocali sono intrinsecamente dati biometrici, richiamando la relativa definizione contenuta nell'art. 4(14) GDPR.

Dato che alcuni VVA hanno la capacità e la specifica funzione di identificare univocamente gli utenti solo in base alla loro voce, attraverso un metodo che si avvale della creazione di modelli di voce (c.d. *voice model recognition* o *voiceprint recognition*), il trattamento dei dati vocali in questi casi richiederà il consenso esplicito della/e persona/e interessata/e (art. 9, par. 2, lett. a) GDPR). Nell'ottenere il consenso degli interessati i titolari del trattamento dovranno rispettare le condizioni dell'art. 7 GDPR e, come chiarito nel Considerando 32 GDPR, dovrebbero offrire un metodo di identificazione alternativo alla biometria, in ossequio alla natura libera del consenso.

Sempre con riferimento alle applicazioni che utilizzano sistemi di *voice model recognition*, si profila il rischio concreto che i VVA operino la registrazione della voce di tutte le persone

che parlano nell'ambiente interessato, al fine di riconoscere, attraverso il metodo del confronto con il modello di voce creato, la voce dello specifico e solo utente deputato a pronunciare la parola chiave di accensione del dispositivo. Le Linee Guida, pur ammettendo la necessità (ove regolarmente dichiarata ed assentita) per l'utente di essere vocalmente riconosciuto dal VVA, chiariscono che - onde evitare raccolte di dati biometrici che abbiano luogo all'insaputa di terzi ignari interessati - occorrerà privilegiare soluzioni tecniche di riconoscimento basate sui soli dati dell'utente stesso. Ciò implicherà la necessità di attivare il riconoscimento biometrico solo ad ogni utilizzo che avvenga su iniziativa dell'utente che richieda di volta in volta l'identificazione, e non sulla base di un'analisi permanente delle voci ascoltate dal VVA. In tal senso, l'EDPB suggerisce ad es. che il VVA chieda all'utente se vuole essere identificato e che attenda una risposta positiva per attivare il trattamento biometrico.

Inoltre, molte delle raccomandazioni espresse dall'EDPB evidenziano la necessità di implementare adeguate misure di sicurezza e di rispettare la c.d. *privacy by design* e la *privacy by default*, in ossequio al principio di *accountability* che, come noto, permea l'intero tessuto normativo del GDPR. Ciò richiede che i fornitori e gli sviluppatori di VVA operino scelte idonee in termini appunto di *design* dei dispositivi, considerando *in primis* la necessità di avere o meno un utente registrato per ciascuna delle loro funzionalità. Ad es. per fare una ricerca su Internet, le Linee Guida ritengono che non sia strettamente necessario che l'utente sia registrato. In particolare, l'EDPB evidenzia come *di default*, i servizi che non richiedono un utente identificato non dovrebbero associare alcuno degli utenti identificati ai comandi. Inoltre, un VVA che sia rispettoso della *privacy by default* e *by design* dovrebbe elaborare solo i dati degli utenti per eseguire le richieste degli utenti e non memorizzare né i dati vocali né un registro dei comandi eseguiti. Ancora, i fornitori di VVA dovrebbero sviluppare standard industriali che consentano la portabilità dei dati in conformità con l'art. 20 GDPR e dovrebbero altresì garantire che tutti i dati degli utenti possano essere cancellati su richiesta dell'utente, conformemente all'art. 17 GDPR.

D'altronde, la garanzia dei diritti dell'interessato occupa a sua volta una parte assai sostanziosa delle Linee Guida, che ne vaglia l'applicabilità in concreto. Soprattutto viene dedicata attenzione proprio al “nuovo” diritto alla portabilità dei dati personali, per la piena applicazione del quale, nel contesto di un mercato unico digitale, i progettisti di VVA sono chiamati, secondo l'EDPB, a sviluppare formati comuni che facilitino l'interoperabilità tra i sistemi VVA.

LAVINIA VIZZONI

[https://edpb.europa.eu/system/files/2021-07/edpb\\_guidelines\\_202102\\_on\\_vva\\_v2.0\\_adopted\\_en.pdf](https://edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf)

2021/3(6)CR

### **Le Linee Guida del Garante Privacy italiano sui cookies ed altri strumenti di tracciamento del 10 giugno 2021**

Il 10 giugno 2021 il Garante per la protezione dei dati personali (il “**Garante**”) ha adottato il provvedimento n. 231 – pubblicato sulla Gazzetta Ufficiale n. 163 del 9 luglio 2021 – recante le nuove “Linee guida *cookie* e altri strumenti di tracciamento” (le “**Linee Guida**”). Il provvedimento, che si applica non solo ai *cookie* ma a tutti gli strumenti di tracciamento

attivi e passivi (es. *fingerprinting*), ha confermato sotto diversi aspetti le precedenti posizioni del Garante – espresse in particolare nelle linee guida sui *cookie* del 2014 – e ha introdotto alcune significative novità.

In primo luogo, viene confermata la distinzione tra *cookie* di prima parte (posizionati dal sito web visitato dall'utente) e *cookie* di terze parti (posizionati da siti o web server diversi). Altra classificazione, basata sulla funzione svolta e a cui si collega una diversa disciplina applicabile, è quella dei *cookie* tecnici (necessari per la stessa erogazione del servizio offerto all'utente tramite il sito web), *cookie analytics* (equiparati ai *cookie* tecnici se utilizzati esclusivamente per produrre statistiche aggregate senza la possibilità di risalire all'utente) e *cookie* di profilazione (utilizzati per ricondurre agli utenti specifiche azioni o schemi comportamentali al fine di raggrupparli in *cluster* omogenei così da personalizzare la fornitura del servizio e inviare messaggi pubblicitari mirati, in linea con le preferenze manifestate dall'utente durante la navigazione in rete).

Il Garante ha poi precisato che la normativa applicabile agli strumenti di tracciamento è l'art. 122 del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196, il “**Codice Privacy**”) che ha dato attuazione nel nostro ordinamento alla direttiva 2002/58/CE del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (la “**direttiva ePrivacy**”). Il regolamento (UE) 2016/679 (“**GDPR**”) ha invece un ambito di applicazione residuale limitato ai profili non direttamente disciplinati dall'art. 122 del Codice Privacy. La direttiva ePrivacy, infatti, si configura come *lex specialis* rispetto al GDPR e, pertanto, è destinata a prevalere su quest'ultimo per la parti di potenziale sovrapposizione. Ne deriva un'importante conseguenza, cioè che il trattamento dei dati personali attraverso gli strumenti di tracciamento può avvenire esclusivamente sulla base del consenso salvi i casi per i quali la direttiva ePrivacy stabilisce che il consenso non è necessario – mentre non può fondarsi sulle altre basi giuridiche previste dal GDPR ma non dalla direttiva ePrivacy (tra cui, in particolare, il legittimo interesse).

Il Garante si sofferma poi sulle modalità di acquisizione del consenso online. Un primo riferimento è allo *scrolling* per il quale le Linee Guida, confermando la posizione espressa dall'EDPB (*European Data Protection Board*) nel parere n. 5/2020 del 4 maggio 2020 (su cui v. la notizia [2020/2\(5\)EMC](#), chiariscono che di per sé lo *scrolling* non costituisce un metodo idoneo alla raccolta del consenso, ma può divenire ammissibile se inserito nell'ambito di un processo più articolato tale da assicurare che la scelta dell'interessato sia inequivoca, consapevole, registrabile e documentabile. Altro tema è quello del c.d. *cookie wall* che il Garante definisce un meccanismo vincolante non conforme al requisito di libertà del consenso, salva l'ipotesi nella quale il titolare del sito offra all'interessato la possibilità di accedere ad un contenuto o a un servizio equivalenti senza prestare il proprio consenso all'installazione e all'uso di *cookie* o altri strumenti di tracciamento, aggiungendo tuttavia che occorre valutare caso per caso se il titolare del trattamento offra una simile possibilità di accedere ad un contenuto o un servizio equivalente per il quale non sia necessario accettare l'installazione di *cookie*. Anche questo tema era stato affrontato nel richiamato parere dell'EDPB n. 5/2020 del 4 maggio 2020 (su cui v. la notizia [2020/2\(5\)EMC](#)). Resta peraltro aperta la questione di cosa debba intendersi per “servizio equivalente” e da che punto di vista – oggettivo o soggettivo – debba valutarsi l'equivalenza.

Un'importante novità riguarda il divieto di reiterazione della richiesta di consenso ad ogni accesso dell'utente al sito web, che il Garante definisce “ridondante e invasiva” e come tale lesiva della libertà di scelta dell'interessato. Ci sono solo tre casi in cui la reiterazione è ammessa: (i) mutamento significativo delle condizioni del trattamento; (ii) impossibilità per

il gestore del sito di sapere che un *cookie* è stato già installato (ad esempio perché l'utente ha cancellato i *cookie*); (iii) dopo 6 mesi dalla precedente richiesta.

Il Garante approfondisce infine il principio della *privacy by design e by default* in applicazione del quale il sito web deve essere configurato in modo che al primo accesso dell'utente non sia installato alcun *cookie* e compaia un *banner* contenente alcune informazioni minime sull'utilizzo dei *cookie*. Il *banner* deve rappresentare una discontinuità nella fruizione del servizio in modo che l'utente possa facilmente identificarlo, e deve essere configurato in modo da non ingannare l'utente cercando di forzare o manipolare le sue scelte (ad esempio attraverso l'uso di colori o dimensioni dei caratteri che spingano l'utente a premere il pulsante di accettazione dei *cookie*). In particolare, l'utente deve avere la possibilità di rifiutare agevolmente i *cookie* anche semplicemente chiudendo il *banner* e, in ogni momento, deve essere in grado di modificare le scelte compiute accedendo ad un'apposita sezione del sito. Solo nel caso in cui il sito utilizzi esclusivamente *cookie* tecnici – o *cookie* analitici equiparati a quelli tecnici – non si rende necessario uno specifico banner ma è sufficiente inserire l'informativa per i *cookie* nella *homepage* o all'interno dell'informativa generale del sito.

CHIARA RAUCCIO

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876>

2021/3(7)AF

### **La decisione del Consiglio direttivo della BCE del 12 luglio 2021 di avviare l'analisi del progetto per un "euro digitale".**

Il 14 luglio 2021 il Consiglio direttivo della Banca centrale europea ("**BCE**") ha comunicato la decisione di avviare il progetto per un "euro digitale". Il progetto avrà inizio nel mese di ottobre 2021 con una fase di analisi della durata di due anni.

La fase di analisi verterà sulla configurazione e sulle modalità di distribuzione di un euro digitale, nonché sul relativo impatto sul mercato e sui rischi per la *privacy* e per l'economia dell'area euro. Riguarderà, in aggiunta, le modifiche legislative che potrebbero rendersi necessarie e implicherà il confronto della BCE con i responsabili delle politiche europee. Un nuovo gruppo consultivo di mercato, il *Digital Euro Market Advisory Group* ("**MAG**"), terrà conto dei punti di vista degli utenti e dei distributori, i quali saranno poi discussi anche dal già esistente *Euro Retail Payments Board* ("**ERP**"), che, sin dal 2013, ha lo scopo di favorire l'integrazione, innovazione e competitività dei pagamenti al dettaglio in euro. Al termine, la BCE deciderà circa l'effettivo sviluppo di un euro digitale.

La fase di analisi fa seguito alle precedenti attività della BCE condotte al riguardo, fra cui il "Rapporto su un euro digitale" pubblicato nel quarto trimestre del 2020 ("**Rapporto**"). Nel Rapporto sono stati delineati i principi generali a cui l'ideazione di un euro digitale dovrebbe ispirarsi e i requisiti che dovrebbe soddisfare. Secondo i principi delineati, l'euro digitale dovrebbe rappresentare una passività della banca centrale offerta in forma digitale e dovrebbe fungere da complemento al contante e alle soluzioni di pagamento private. Costituirebbe, quindi, un'altra forma attraverso cui rappresentare l'euro e non una valuta ulteriore. L'emissione, poi, dovrebbe aversi garantendo accessibilità e coesistenza con soluzioni di pagamento private per i pagamenti digitali *retail*, nonché fiducia da parte degli utenti finali. I requisiti sono stati definiti con riferimento sia a specifici scenari che potrebbero motivarne l'emissione, sia ai potenziali effetti che un euro digitale potrebbe avere. In generale, fra tutti,

si hanno sicurezza e solidità; fruibilità; efficienza; cooperazione con gli operatori di mercato; conformità al quadro regolamentare.

Dalla configurazione dell'euro digitale ne dipende il fondamento normativo. A seconda che sia concepito per un impiego circoscritto a determinate fattispecie o per un uso diffuso, la base giuridica sarà diversa. Come evidenziato dal Rapporto, l'alternativa coerente a un impiego diffuso e analogo al contante- che sembrerebbe essere l'ipotesi prevalente- sarebbe data da l'art. 128, co. 1, TFEU e l'art. 16 dello Statuto del SEBC, secondo cui le banconote in euro emesse dall'Eurosistema sono le uniche banconote aventi corso legale nell'Unione. Secondo il Rapporto, l'assenza di un'espressa previsione che escluda la possibilità per l'Eurosistema di emettere strumenti aventi corso legale diversi dalle banconote e la mancanza di disposizioni circa il mezzo e il formato attraverso cui dovrebbe avvenire l'emissione delle *euro banknotes* consentirebbero margini di discrezionalità nell'emissione di un euro digitale.

Le sfide tecnologiche poste da un euro digitale sono state valutate nel successivo lavoro di sperimentazione condotto dall'Eurosistema congiuntamente a esponenti del mondo accademico e del settore privato. Per ciascun *work stream*, diversi assetti di emissione e distribuzione, centralizzati e non, sono stati presi in esame. In particolare, si sono considerate, in combinazione o alternativamente, sia soluzioni basate su infrastrutture esistenti e su sistemi *account-based*, sia tecnologie innovative e sistemi *distributed ledger-based*. In aggiunta, sono state prese in esame soluzioni *offline*. La valutazione è stata condotta rispetto a quattro ambiti: tecnologia per un euro digitale (*digital euro ledger*); *privacy* e contrasto al riciclaggio di denaro; limiti alla circolazione di un euro digitale; accessibilità da parte degli utenti. Dalle risultanze ottenute è emerso che non vi dovrebbero essere ostacoli allo sviluppo di un euro digitale per nessuna delle aree considerate. Le evidenze emerse costituiranno una prima base per la fase di analisi.

La fase di indagine terrà conto anche della consultazione pubblica condotta in parallelo al lavoro di sperimentazione. Dalle risposte ottenute è emerso che l'aspetto che i cittadini e i professionisti ritengono più rilevante nello sviluppo di un euro digitale è la *privacy*, anche se altrettanta rilevanza è stata attribuita alla prevenzione di attività illecite. Particolare attenzione è stata dedicata anche al tema della sicurezza e dell'accessibilità, nonché alla possibilità di utilizzare l'euro digitale senza costi aggiuntivi e *offline*. Rispetto alle modalità di distribuzione, è emersa una preferenza per un'integrazione dell'euro digitale negli attuali sistemi bancari e di pagamento, con, però, anche il desiderio di godere di servizi aggiuntivi.

Alice Filippetta

<https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.it.html>  
[https://www.ecb.europa.eu/paym/digital\\_euro/mag/shared/files/digital\\_euro\\_stakeholder\\_engagement.pdf](https://www.ecb.europa.eu/paym/digital_euro/mag/shared/files/digital_euro_stakeholder_engagement.pdf)  
[https://www.ecb.europa.eu/pub/pdf/other/Report\\_on\\_a\\_digital\\_euro~4d7268b458.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf)

2021/3(8)FP

**La Repubblica di El Salvador adotta il Bitcoin come moneta avente corso legale nel Paese (la “Ley Bitcoin” dell’8 giugno 2021).**

Attraverso il decreto 57/2021 del 9 giugno 2021 (noto come “**Ley Bitcoin**”), l'Assemblea Legislativa della República de el Salvador ha introdotto il Bitcoin come “moneda de curso

legal” rendendo, di fatto, lo Stato centroamericano il primo paese al mondo a adottare la più diffusa cryptomoneta come valuta domestica. Il provvedimento, già preannunciato dal Presidente Nayid Bukele qualche settimana prima della sua presentazione, avrà efficacia decorsi 90 giorni dalla votazione della proposta in Parlamento e, segnatamente, il 7 settembre 2021. Oltre a ragioni legate all’opportunità di attrarre investimenti stranieri, le caratteristiche del sistema economico e finanziario dello Stato centroamericano sono state alla base di una scelta così radicale ed innovativa, nonché della larga maggioranza con la quale essa è stata votata in Parlamento (64 voti su 84 totali).

El Salvador appartiene a quegli ordinamenti che nell’esercizio della propria sovranità monetaria decidono di riconoscere – in via esclusiva o in aggiunta ad una o più valute locali – corso legale ad una moneta emessa da un ordinamento straniero. La scelta risiede perlopiù nella volontà di una economia in via di sviluppo di incrementare gli scambi commerciali con l’estero attraverso una riduzione del rischio di cambio, che altrimenti disincentiverebbe investitori stranieri nel fare affidamento a valute più deboli (come nel caso del Colon salvadoregno). Nel caso della Repubblica centroamericana, già prima del 2001, questo obiettivo era comunque perseguito attraverso un regime di cambio fisso fra la valuta locale ed il dollaro USA; a seguito poi dell’entrata in vigore della “Ley de Integración Monetaria” (Ley 201 del 30 novembre 2000), è stato poi riconosciuto al dollaro americano valore di moneta avente corso legale nello Stato. La situazione di costante instabilità politica e l’alto tasso di criminalità della República non ha però consentito di raggiungere gli effetti sperati, producendo al contrario un aumento vertiginoso dell’inflazione ed ampliando il divario di ricchezza fra le diverse fasce della popolazione. L’adozione della valuta americana come moneta domestica implicava, inoltre, una significativa riduzione dei margini di manovra del Banco Central de Reserva de el Salvador, poiché rendeva lo Stato dipendente dalle decisioni di politica monetaria intraprese dall’organo che regola l’emissione della valuta americana (il Federal Reserve System). La crisi derivante dalla diffusione della pandemia da COVID-19 ha poi ulteriormente acuitizzato il problema della dipendenza dalla sovranità monetaria di uno Stato estero. Per far fronte alla crisi dell’economia reale indotta dalle chiusure forzate delle attività non essenziali, il FED ha iniettato nel sistema finanziario dosi di liquidità elevata che hanno determinato, nei Paesi con economie “satellite” di quella americana, un aumento incontrollabile dell’inflazione.

La nuova legge si colloca così - per espressa menzione all’interno dei considerando iniziali - sotto l’egida dell’art. 102 della Constitución de la República, la quale attribuisce allo Stato il compito di promuovere e sostenere l’iniziativa privata, generando le condizioni necessarie per accrescere la ricchezza nazionale a beneficio del maggior numero di abitanti possibile. Il riconoscimento del Bitcoin come moneta avente corso legale nasce difatti come manovra di finanza inclusiva, tenuto conto del fatto che circa il 70% della popolazione non ha accesso a servizi finanziari tradizionali e che una parte significativa degli introiti finanziari dello Stato (attorno al 22% del PIL) provengono da proventi inviati da cittadini salvadoregni al proprio Paese d’origine. Su queste basi, la legge dispone la regolamentazione del Bitcoin come moneta a corso legale, con potere liberatorio senza alcuna restrizione, senza alcun limite in ogni transazione e a qualsiasi titolo che le persone fisiche o giuridiche, pubbliche o private richiedano di compiere (art. 1). A livello di mercato interno, il Bitcoin potrà essere impiegato per esprimere i prezzi di beni e servizi (art. 3), per adempiere ad obblighi tributari (art. 4), con obbligo per ogni agente economico di accettare la cryptovaluta come forma di pagamento (art. 7). Le disposizioni della Ley Bitcoin assumono dunque, ad oggi, carattere meramente programmatico, richiamando il compito dello Stato di fornire alternative che consentano agli utenti di effettuare transazioni in Bitcoin, di garantire convertibilità automatica ed istantanea fra Bitcoin e dollari (art. 8), di promuovere la formazione e i

meccanismi di accesso della popolazione a transazioni in Bitcoin (art. 12), oltre ad affidare all'Esecutivo, al Banco Central e alla Sovrintendenza al Sistema Finanziario la competenza ad adottare i regolamenti attuativi (artt. 10 e 11). Prima dell'entrata in vigore della legge, lo Stato garantirà inoltre la convertibilità automatica ed istantanea fra dollaro e Bitcoin attraverso la creazione di un trust nella Banca di Sviluppo di El Salvador (art. 14). La legge produce infine, per espressa previsione, efficacia retroattiva, riconoscendo la facoltà di adempiere in Bitcoin ogni obbligazione pecuniaria in essere espressa in dollari (art. 13).

Al netto delle implicazioni “politiche” che questa decisione assume – rendendo el Salvador frontrunner di un esperimento che sarà verosimilmente emulato da parte di altri ordinamenti – la scelta di adottare il Bitcoin come valuta domestica produce rilevanti implicazioni sul versante della politica monetaria e dell'ordine giuridico interno dello Stato. Sotto il primo aspetto, è noto che una delle principali caratteristiche della cryptovaluta è quella per cui il suo valore non è fissato o influenzato dalle scelte di uno Stato, una banca centrale o un intermediario finanziario (moneta FIAT), ma dipende – in larga parte – da “criterios de libre mercado” (così il considerando V della Ley Bitcoin), secondo un sistema cd. decentralizzato. In buona sostanza, la sua produzione ed immissione nel sistema non dipende da una programmazione di un ente centrale in considerazione di obiettivi di politica monetaria, bensì dalla progressione dell'attività di mining scandita da un algoritmo (fino all'ammontare massimo di 21 milioni previsto dal protocollo Bitcoin entro il 2140). Se dunque, da un lato, il fondamento di politica economica che ha sorretto la scelta della República de el Salvador è stato quello di sottrarsi all'influenza prodotta dalle decisioni monetarie del FED, dall'altro, il riconoscimento di corso legale al Bitcoin non comporta alcun recupero di sovranità monetaria da parte dello Stato, poiché le decisioni del Banco Central hanno una più limitata capacità di incidere sull'economia reale rispetto a fattori legati all'andamento di mercato della cryptovaluta. Sotto un secondo aspetto, l'adozione del Bitcoin come unità di conto e mezzo di scambio comporta l'obbligo del creditore di accettare la cryptovaluta come metodo di pagamento per estinguere il debito pecuniario (salvo la convenzione di clausole cd. “effettivo” che riconoscono efficacia estintiva ad una particolare moneta in soluzione): l'accettazione viene effettuata al valore nominale pieno della moneta sulla base del principio nominalistico. Il riconoscimento di questa *facultas solutionis* attraverso il pagamento in Bitcoin non esclude, tuttavia, la possibilità di impiego di altre valute accettate come aventi corso legale nello Stato (il dollaro, il Colon salvadoregno etc.).

Come ricordato, il provvedimento legislativo costituisce, allo stato attuale, una mera base programmatica, la cui effettività sarà da misurarsi attraverso i diversi atti e regolamenti che andranno a definire le misure attuative. Deve tuttavia registrarsi un primo importante arresto da parte della Banca Mondiale che, a fronte di una richiesta di assistenza formulata dal governo salvadoregno nell'implementazione del progetto, ha comunicato il proprio dissenso rispetto all'operazione. In particolare, il rifiuto poggia sui dubbi espressi dalla Banca Mondiale circa la trasparenza del processo e la sostenibilità energetica del mining. Studi recenti (*Cambridge Bitcoin Electricity Consumption Index*, 2021) mostrano che l'estrazione di Bitcoin produce un impatto in termini di consumo annuale di energia elettrica superiore a quello dell'Argentina, data la potenza di calcolo elevatissima richiesta dai computer che effettuano attività di mining. Al rifiuto di cooperazione da parte della Banca Mondiale ha fatto poi eco l'avvertimento del Fondo Monetario Internazionale secondo cui l'adozione del Bitcoin come moneta a corso legale solleva una serie di questioni macroeconomiche, finanziarie e legali che richiedono un'analisi molto attenta, poiché le cryptovalute possono comportare rischi significativi se non vengono adottate misure normative efficaci.

FEDERICO PISTELLI

<https://www.diarioofficial.gob.sv/diarios/do-2021/06-junio/09-06-2021.pdf>

2021/3(9)AN

### **Il provvedimento del 22 luglio 2021 del Garante Privacy nei confronti di Deliveroo per il trattamento dei dati personali dei riders**

Con provvedimento n. 285 del 22 luglio 2021 il Garante per la protezione dei dati personali (il “**Garante**”) ha emesso un’ ordinanza di ingiunzione nei confronti della società Deliveroo Italy S.r.l. ( “**Deliveroo**”), con riferimento al trattamento dei dati personali dei ciclo fattorini, c.d. *riders* (il “**Provvedimento**”).

Deliveroo - come è noto - è una società che svolge, per mezzo di una piattaforma digitale, un’ attività di consegna di cibo ed altri beni, forniti da molteplici esercenti, avvalendosi di personale a ciò dedicato (i c.d. *riders*).

Sulla base degli elementi di fatto relativi al modello di organizzazione del lavoro (che avviene in maniera integralmente automatizzata attraverso una app che ogni *rider* deve scaricare sul proprio dispositivo mobile), riscontrati nella fase istruttoria, il Garante ha ritenuto il trattamento dei dati personali dei *riders* posto in essere da Deliveroo illegittimo per:

- (i) violazione dei principi di liceità, correttezza, minimizzazione e limitazione della conservazione, in relazione all’art. 5 lett. a) c) ed e) del Regolamento UE 2016/679 (“**GDPR**”);
- (ii) violazione delle regole in materia di informativa (art. 13 GDPR) e di trattamenti automatizzati, con particolare riferimento all’obbligo di adottare delle misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell’interessato (art. 22, par.3 GDPR);
- (iii) violazione delle regole in materia di protezione dei dati sin dalla progettazione e per impostazione predefinita (*privacy by design e by default*, art. 25 GDPR);
- (iv) violazione delle regole sulla tenuta del Registro dei trattamenti (art. 30, par.1, lett. c), f) e g) GDPR);
- (v) mancata adozione delle misure di sicurezza nel trattamento dei dati (art. 32 GDPR);
- (vi) violazione delle regole in materia di valutazione di impatto del trattamento (art. 35 GDPR), anche in considerazione delle tecnologie utilizzate;
- (vii) mancata comunicazione - fino al 31 maggio 2019 - dei dati di contatto del responsabile della protezione dei dati all’Autorità di controllo (art. 37, par. 7 GDPR);
- (viii) violazione delle regole in materia di trattamento dei dati personali nell’ambito dei rapporti di lavoro (art. 88 GDPR);
- (ix) mancata adozione delle garanzie in materia di controllo a distanza (art. 114 del Codice in materia di protezione dei dati personali, recante disposizioni per l’adeguamento dell’ordinamento nazionale al GDPR, d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101).

In conseguenza di tale accertamento, il Garante ha, pertanto, ingiunto a Deliveroo, in base a quanto previsto dall’ art. 58 par. 2 lett. d) GDPR, di:

- (i) predisporre correttamente entro 60 giorni dal ricevimento del Provvedimento, i documenti in materia di informativa, fornendo precise indicazioni ai *riders* in

merito al funzionamento del sistema di assegnazione degli ordini attualmente in uso (comprese le indicazioni sulla tipologia dei dati trattati e sui trattamenti dei dati già raccolti dal sistema di elaborazione delle statistiche), il registro dei trattamenti e la valutazione di impatto;

- (ii) individuare correttamente, entro 60 giorni dal ricevimento del Provvedimento, i tempi di conservazione dei dati;
- (iii) individuare entro 60 giorni dal ricevimento del Provvedimento, le misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno con riferimento al diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione, in relazione ai trattamenti automatizzati, compresa la profilazione, effettuati mediante la piattaforma;
- (iv) individuare misure appropriate volte alla verifica periodica della correttezza ed accuratezza dei risultati dei sistemi algoritmici, anche al fine di garantire che sia minimizzato il rischio di errori e conformarsi a quanto stabilito dall'art. 47-quinquies, d. lgs. n. 81/2015 (come modificato dal Decreto legge 3 settembre 2019, n. 101, convertito con modificazioni in Legge 2 novembre 2019, n. 128 – recante norme specifiche a tutela del lavoro svolto mediante piattaforme digitali e, in particolare, dell'attività lavorativa dei c.d. *riders*) in materia di divieto di discriminazione, accesso alla piattaforma ed esclusione dalla piattaforma; detta attività dovrà essere avviata dalla Società entro 60 giorni dal ricevimento del Provvedimento e la verifica dovrà essere conclusa entro i successivi 90 giorni;
- (v) individuare misure appropriate volte ad introdurre strumenti per evitare usi impropri e discriminatori dei meccanismi reputazionali basati su *feedback*, con obbligo di ripetere la verifica ad ogni modifica dell'algoritmo, relativamente all'utilizzo dei *feedback* per il calcolo del punteggio; detta attività dovrà essere avviata dalla Società entro 60 giorni dal ricevimento del Provvedimento e la verifica dovrà essere conclusa entro i successivi 90 giorni;
- (vi) applicare, entro 60 giorni dal ricevimento del Provvedimento, i principi di minimizzazione e di *privacy by design* e *by default*, in relazione al trattamento dei dati dei *riders*;
- (vii) individuare i soggetti autorizzati ad accedere ai sistemi, in qualità di supervisor, con visibilità non limitata su base territoriale, definendo ipotesi predeterminate e specifiche finalità che rendano necessario tale accesso e adottando le misure appropriate per assicurare la verifica di tali accessi;
- (viii) adempiere, entro 60 giorni dal ricevimento del Provvedimento, a quanto previsto dall'art. 4, comma 1, l. 20.5.1970, n. 300, con riferimento al divieto di controllo a distanza dei lavoratori.

Il Garante ha inoltre applicato ai danni ddi Deliveroo una sanzione pecuniaria di Euro 2.500.000.

ARIANNA NERI

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9685994>

2021/3(10)CM**Il pronunciamento del 28 maggio 2021 della Suprema Corte del Popolo della Repubblica Popolare Cinese sul valore probatorio dei dati registrati su blockchain**

Il 28 maggio 2021, la Suprema Corte del Popolo della Repubblica Popolare Cinese ha pubblicato le *Regole sul Contenzioso Online dei Tribunali del Popolo* (《人民法院在线诉讼规则》, in seguito le ‘Regole’). Le Regole, composte di 39 articoli ed entrate in vigore il 1° agosto 2021, illustrano i principi fondamentali, l’ambito d’applicazione e le condizioni per l’accesso ai contenziosi online e forniscono informazioni sulle fasi della procedura, la modalità di svolgimento delle udienze, la pubblicazione e l’esecuzione delle sentenze, l’archiviazione dei casi. Particolarmente innovativa, risulta la previsione della revisione dell’autenticità delle prove giudiziali presentate dalle parti mediante uso di tecnologia *blockchain*. Si prevede che le prove elettroniche presentate attraverso la tecnologia *blockchain* e tecnicamente verificate si presumeranno esenti da manomissioni dopo essere state caricate sulla catena, a meno che non vi siano prove contrarie sufficienti per ribaltare la presunzione (Articolo 16). Le Regole forniscono inoltre indicazioni su come rivedere l’autenticità delle prove elettroniche archiviate utilizzando la tecnologia *blockchain*, compreso come determinare se le prove elettroniche sono state alterate prima di essere archiviate sulla catena (Articoli 17-19). La Suprema Corte, nel comunicato ufficiale, ha affermato che le “prove *blockchain*” porteranno maggiore trasparenza, sicurezza, tracciabilità ed efficienza alle controversie online in Cina, dimostrando quindi di fare pieno affidamento su questa tecnologia.

CORRADO MORICONI

<http://www.court.gov.cn/zixun-xiangqing-309551.html>[http://english.court.gov.cn/2021-06/18/content\\_37545136.htm](http://english.court.gov.cn/2021-06/18/content_37545136.htm)2021/4(1)FBe**Il recepimento in Italia delle direttive (UE) 2019/770 e 2019/771 relative a determinati aspetti dei contratti di fornitura di contenuti e servizi digitali e a determinati aspetti dei contratti di vendita di beni di consumo.**

Con i D.Lgs. 4 novembre 2021, nn. 170 e 173, il legislatore italiano ha dato recepimento alle direttive UE del 20 maggio 2019, nn. 2019/771 e 2019/770, rispettivamente relative a determinati aspetti dei contratti di vendita dei beni di consumo e a talune prescrizioni concernenti i contratti di fornitura di contenuti o servizi digitali (di seguito anche solo “**dir. 771**” e “**dir. 770**”).

Le due direttive si collocano all’interno della medesima strategia per il raggiungimento del mercato unico digitale. Pur differenziandosi per l’ambito di applicazione, esse condividono la finalità di «contribuire al corretto funzionamento del mercato interno garantendo nel contempo un livello elevato di protezione dei consumatori», che perseguono imponendo agli Stati membri un livello di massima armonizzazione (artt. 1 e 4 di entrambe le direttive). Ciò implica che, in fase di recepimento, ai legislatori nazionali sia precluso mantenere «disposizioni divergenti» da quelle delle direttive o introdurne di ulteriori per garantire al consumatore un livello di tutela diverso.

I profili di «digitalizzazione» del mercato unico si colgono già nei profili definatori della direttiva dedicata alla vendita di beni di consumo, che integra la nozione di «bene» fino a ricomprendervi qualsiasi bene mobile materiale incorporante o interconnesso con un contenuto digitale o un servizio digitale la cui mancanza «impedirebbe lo svolgimento delle funzioni proprie del bene» (art. 2, n. 5, lett. b, testualmente riproposto all'interno dell'art. 128, co. 2, lett. e, c. cons., come sostituito per effetto del d.lgs. 173/2021).

I criteri di conformità al contratto fissati dalla dir. 771 e la responsabilità del venditore per la loro assenza sono declinati alla luce del più esteso ambito oggettivo di applicazione della dir. 771 rispetto alla precedente direttiva CE 1999/44, espressamente abrogata. I requisiti della funzionalità, compatibilità, interoperabilità, sicurezza e durabilità richiesti affinché i beni ai quali si applicano le previsioni della dir. 771 possano superare positivamente il giudizio di conformità richiedono indubbiamente un ripensamento che muova dalla diversa natura del «bene digitale». La soddisfazione del giudizio di conformità, però, pare anche assumere contorni di durata per i beni di quest'ultima categoria, perché si impone al venditore di fornire e assicurare la corretta installazione degli aggiornamenti previsti dal contratto e necessari per mantenere la conformità nei due anni successivi alla consegna.

Nonostante l'estensione dell'applicazione della disciplina della vendita di beni di consumo ai beni con elementi digitali, la dir. 771, per l'espressa esclusione operata dall'art. 1, non si applica ai contratti di fornitura di un contenuto digitale o di un servizio digitale, regolati invece dalla direttiva «gemella», la dir. 770. La necessità di coordinamento tra la dir. 770 e la dir. 771 è evidente, ma il legislatore italiano che ha curato il recepimento di ciò non ha dimostrato particolare consapevolezza, limitandosi in buona misura a trasportare all'interno del codice del consumo le previsioni delle due direttive.

Segnatamente, l'art. 1 D.Lgs. 173/2021 introduce, dopo il capo I del titolo III della parte IV c. cons., il nuovo capo I-bis (artt. 135 *octies* ss. c. cons.), relativo ai contratti di fornitura di contenuto digitale e di servizi digitali, mentre l'art. 1 D.Lgs. 170/2021 sostituisce integralmente il capo I del titolo III della parte IV del codice del consumo (artt. 128 ss. c. cons.), al fine di adeguarlo alle novità introdotte dalla seconda. Entrambe le modifiche al c. cons. acquistano efficacia a decorrere dal 1° gennaio 2022, ai sensi degli artt. 2 dei decreti richiamati, con l'unica differenza che le disposizioni di cui ai nuovi artt. 128 ss. si applicheranno ai soli contratti conclusi successivamente a tale data, mentre quelle di cui al nuovo capo I bis saranno applicate a tutte le forniture di contenuto digitale o di servizi digitali che avverranno a decorrere dalla presa di efficacia delle disposizioni, a prescindere dalla data di conclusione del contratto, con esclusiva eccezione delle disposizioni di cui agli artt. 135 *quindecies* e 135 *vicies semel*, relativi al diritto di regresso del professionista e alla modifica del contenuto digitale o del servizio digitale, applicabili ai soli contratti conclusi dopo il 1 gennaio 2022.

I nuovi artt. 128 – 135 *septies* c. cons. ricalcano pedissequamente la struttura e i contenuti della dir. 771, il cui ambito di applicazione oggettivo è solo parzialmente coincidente con quello della dir. 1999/44/CE, dalla stessa abrogata. La «vendita» di beni di consumo si conferma essere una disciplina applicabile in via transtipica alle relazioni b2c in fattispecie contrattuali che poco o nulla hanno a che vedere con la vendita in senso tecnico, ma che ad essa sono espressamente equiparate (così, il nuovo art. 128 c. cons., stabilisce che, ai fini dell'applicazione del capo a cui dà apertura, alla compravendita «sono equiparati i contratti di permuta e di somministrazione nonché quelli di appalto, d'opera e tutti gli altri contratti comunque finalizzati alla fornitura di beni da fabbricare o produrre». L'ampliamento del perimetro di operatività della materia, che si riflette immediatamente sui profili definatori di cui al nuovo art. 128 c. cons. e che determina una più articolata configurazione della responsabilità del venditore (ex artt. 130 e 133 c. cons.) è sostanzialmente collegato

all'allargamento dell'oggetto del contratto concluso tra professionista e consumatore, che può ora riguardare anche beni con elementi digitali.

Con riguardo a quest'ultima categoria di beni, il venditore è chiamato a rispondere di qualsiasi difetto di conformità del contenuto digitale o del servizio digitale che si verifica o si manifesta entro due anni dalla consegna, ovvero per il maggiore arco temporale per il quale il contratto concluso preveda la fornitura del contenuto digitale o del servizio digitale (art. 133, co. 2 c. cons.); deve altresì, per il medesimo lasso temporale, «tenere informato il consumatore sugli aggiornamenti disponibili, anche di sicurezza, necessari al fine di mantenere la conformità» (art. 130, co. 2 c. cons.).

È peraltro verosimile ipotizzare che la possibilità di instaurare un giudizio comparativo tra le qualità ontologiche del bene e le qualità deontologiche dello stesso anche a seguito dell'errata installazione, seppur con esclusivo riferimento ai casi previsti dal nuovo art. 131 c. cons., porterà il venditore di beni con elementi digitali ad adottare particolari cautele – almeno informative – relative alla fase di installazione.

Il diritto di regresso riconosciuto al venditore «responsabile nei confronti del consumatore a causa di un difetto di conformità imputabile ad un'azione o ad un'omissione di una persona nell'ambito dei passaggi precedenti della medesima catena contrattuale distributiva» copre, ai sensi del nuovo art. 134 c. cons., anche la circostanza in cui la mancanza di conformità derivi dall'omessa fornitura degli aggiornamenti di beni con elementi digitali.

Da un punto di vista sostanziale, il recepimento degli artt. 6, 7 e 10 dir. 771 nei nuovi artt. 129 e 133 c. cons. rappresenta la novità con maggiore impatto sistematico.

Nonostante il legislatore italiano non si sia cimentato in sforzi tesi a chiarire la natura della responsabilità del venditore, la formulazione dell'art. 10, co. 1, dir. 771, a cui fa eco l'art. 133, co. 1., c. cons., secondo la quale «il venditore è responsabile nei confronti del consumatore» dei difetti di conformità sembra ormai inequivocabilmente contraddistinguere un'obbligazione del venditore di consegnare beni conformi.

La disarticolazione dei criteri di conformità su due livelli, uno soggettivo e uno oggettivo, operata a livello interno attraverso i commi 2 e 3 del nuovo art. 129 c. cons., poi, milita nella medesima direzione: oltre a parametri soggettivi di conformità, che si riferiscono alle qualità della *res* specificamente oggetto del contratto o di trattativa, al fine di essere giudicato conforme il bene deve presentare anche caratteristiche che il legislatore europeo eleva ad elementi integrativi della conformità sulla base di un'oggettivazione della ragionevole aspettativa del consumatore rispetto alla loro presenza nel bene acquistato. Rientrano tra i parametri oggettivi di conformità l'idoneità agli scopi per i quali si impiegano normalmente beni dello stesso tipo, la corrispondenza all'eventuale campione o modello messo a disposizione dal venditore, la presenza del corredo di accessori e istruzioni e quella delle qualità ragionevolmente attesi dal consumatore sulla base della natura del bene e delle dichiarazioni pubbliche rese dai professionisti intervenuti nella commercializzazione del bene.

Il grado di oggettività assunto dall'aspettativa del consumatore provocata dalle dichiarazioni pubbliche dei professionisti emerge altresì dalla disposizione di cui all'art. 135 *quinquies* c. cons., che recepisce l'art. 17 della dir. 771 ed ha per oggetto le garanzie convenzionali. Esso infatti stabilisce, nell'inciso conclusivo del primo comma, che la garanzia convenzionale vincola secondo le condizioni indicate nella pubblicità ad essa relativa se queste sono più vantaggiose rispetto a quelle effettivamente contenute nella dichiarazione di garanzia.

La norma di chiusura, l'art. 135 *septies* c. cons., che svolge il ruolo di coordinamento con le altre «altre disposizioni» dell'ordinamento svolta sino ad ora dall'art. 135 c. cons., segna forse il più significativo punto di rottura con il passato. Allineandosi con l'obiettivo della

massima armonizzazione fissato dal legislatore comunitario (*ex art. 4 dir. 771*), la norma eclissa il c.d. principio di maggior tutela del consumatore ricavabile dalla formulazione del previgente art. 135 c. cons., in forza del quale parte della dottrina riteneva che, a fronte della consegna di un bene non conforme, si configurasse un concorso alternativo di rimedi tale da lasciare al consumatore la possibilità di scegliere discrezionalmente se appellarsi alla disciplina del codice civile in presenza di un difetto di conformità rientrante altresì nella nozione di vizio, ovvero invocare i rimedi specificamente consumeristici. La nuova norma contenuta nel primo comma dell'art. 137 *septies* c. cons. rinvia infatti alle disposizioni del codice civile, facendo espresso riferimento a quelle dedicate a «formazione, validità ed efficacia dei contratti, comprese le conseguenze della risoluzione del contratto e il diritto al risarcimento del danno», ma il medesimo articolo, al secondo comma, ha cura di escludere che per tutto quanto regolato dal capo dedicato alla vendita di beni di consumo, possano trovare applicazione norme tese a garantire al consumatore un diverso livello di tutela. Per l'effetto, al consumatore si impedisce di eludere la gerarchia rimediale rigida che, salvo specifiche eccezioni, subordina la riduzione del prezzo e la risoluzione del contratto al previo infruttuoso esperimento dei rimedi conservativi di primo grado.

L'innalzamento del livello di tutela del consumatore rimane, in realtà, possibile ai sensi dell'art. 135 *sexies* c. cons. che, nello stabilire il carattere imperativo delle disposizioni, da una parte sanziona con la nullità tutti gli accordi precedenti alla comunicazione del difetto di conformità che limitino la responsabilità del venditore, dall'altra, però, consente che l'autonomia privata dei contraenti possa in qualsiasi tempo trovare spazio nella direzione opposta, ossia nel senso di adottare, all'interno della singola contrattazione b2c, pattuizioni volte a rafforzare la posizione del consumatore.

Ne scaturisce la necessità di interrogarsi su quali siano i criteri sulla base dei quali stabilire in termini oggettivi quando le condizioni contrattuali assicurino una «maggior tutela» e siano perciò da ritenersi valide, perché il giudizio circa il livello di soddisfacimento del consumatore rispetto all'utilità prefissata con la conclusione del contratto potrebbe rispondere ad una valutazione di interessi concreti che, ove rimessa all'autonomia negoziale anche in ordine ai rimedi esperibili, difficilmente potrebbe giustificare una valutazione sul merito da parte dell'autorità giurisdizionale.

Alla gerarchia verticale tra i rimedi esperibili dal consumatore è dedicato il nuovo art. 135 *bis* c. cons., che riconosce il diritto del consumatore alla riduzione proporzionale del prezzo o alla risoluzione del contratto solo quando l'inadempimento del venditore rispetto all'obbligo di conformità acquisti connotati di gravità o irreversibilità tali da giustificare un intervento sul sinallagma (art. 135 *bis*, co. 4, c. cons.), peraltro negando (art. 135 *bis*, co. 5, c. cons.) l'accesso al rimedio perentorio in tutti i casi in cui la lieve entità del difetto di conformità escluda quell'importanza dell'inadempimento che, *ex art. 1455 c.c.*, legittima la risoluzione.

Ferma restando la possibilità che il venditore rifiuti il ripristino della conformità se la riparazione o la sostituzione sono impossibili o se i costi da sopportare a tal fine non rispettano il principio di proporzionalità e impregiudicate sia la tutela risarcitoria ai sensi del codice civile, così come l'autotutela dilatoria (art. 135 *bis*, co. 6, c. cons.), la libertà del consumatore è chiaramente circoscritta alla possibilità di scelta tra la riparazione o la sostituzione del bene. Anche tale opzione è tuttavia orientata dal criterio della proporzionalità del rimedio, da valutarsi, per espressa previsione normativa, con particolare riguardo alla convenienza dell'alternativa per il consumatore, al valore che il bene avrebbe in assenza del difetto di conformità e alla sua entità.

I successivi artt. 135 *ter* e *quater* sono rispettivamente dedicati alle modalità di esercizio dei rimedi di primo e secondo grado. Rispetto ai primi, il disposto attiene sostanzialmente alle

modalità di esecuzione dell'intervento manutentivo. Per i secondi, invece, va segnalata indubbiamente una definitiva presa di posizione del legislatore europeo sulla configurazione assunta dal rimedio perentorio: la risoluzione è conseguenza dell'esercizio di un diritto potestativo del consumatore, esercitato mediante una dichiarazione unilaterale diretta al venditore e «contenente la manifestazione di volontà di risolvere il contratto di vendita» e, qualora il difetto di conformità riguardi solo alcuni dei beni oggetto del contratto, può essere parziale.

Il legislatore italiano ha mantenuto fede al testo della direttiva tacendo, invece, sulle modalità con cui il consumatore può ottenere la riduzione del prezzo. Ad essa è dedicato solo il primo comma dell'art. 135 *quater*, che richiama nuovamente la proporzionalità rispetto alla diminuzione di valore conseguenza del difetto di conformità come unità di quantificazione della riduzione, ma nulla dice circa le modalità operative con cui ottenerla.

Il recepimento della direttiva «gemella» (dir. 770) ha invece portato alla creazione del capo I bis all'interno del titolo III della parte IV c. cons., composto dagli artt. 135 *octies* - 135 *vicies ter*.

Da un punto di vista strutturale, l'omozigosi tra i due plessi di nuova introduzione all'interno del codice del consumo è pressoché totale. L'introduzione di un articolato che ambisce ad estendere le tutele consumeristiche previste per il difetto di conformità, con i dovuti adattamenti, ai «contratti di fornitura di contenuto digitale o di servizi digitali conclusi tra consumatore e professionista» (ex art. 135 *octies* c. cons.) è significativa rispetto all'avvertita necessità di interventi regolatori che tengano in considerazione la digitalizzazione delle transazioni e contribuiscano alla creazione di un mercato unico digitale in cui siano evitati approfittamenti degli squilibri di potere a danno dei consumatori ed entro il quale gli operatori dell'Unione possano agire con sufficiente certezza e prevedibilità delle conseguenze (tra gli altri, Considerando 3, 6, 8 e art. 1 dir. 770).

Da qui si spiega agevolmente la scelta del legislatore europeo di caratterizzare anche la dir. 770 come provvedimento di armonizzazione massima e quella del legislatore nazionale di riproporre una norma di coordinamento delle disposizioni del nuovo capo sovrapponibile *in toto* a quella con cui si conclude il capo dedicato alla vendita di beni di consumo: invero, anche l'art. 135 *vicies ter* c. cons. preclude di applicare altre disposizioni aventi l'effetto di garantire al consumatore un livello di tutela diverso per quanto già disciplinato dalle regole settoriali. Peraltro, anche nel caso di contratti di fornitura di contenuti o servizi digitali, il carattere imperativo delle disposizioni fa comunque salva la possibilità di pattuire condizioni contrattuali di maggior favore per il consumatore (art. 135 *vicies bis* c. cons.).

L'integrazione vicendevole tra le norme che danno recepimento alle due direttive, espressamente auspicata dal Considerando 20 della dir. 770, si coglie con il solo raffronto dell'ambito di applicazione delle due e dalle esclusioni che queste operano.

Ciò che il nuovo art. 128, co. 3, c. cons. ha espressamente cura di escludere dalla propria sfera di operatività ricade invece all'interno del perimetro dell'art. 135 *octies* c. cons., esteso a «qualsiasi contratto in cui il professionista fornisce, o si obbliga a fornire, un contenuto digitale o un servizio digitale al consumatore e il consumatore corrisponde un prezzo o si obbliga a corrispondere un prezzo» (co. 3), inclusi i contratti con i quali (co. 4) «il professionista fornisce o si obbliga a fornire un contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si obbliga a fornire dati personali al professionista» quando questi non sono esclusivamente funzionali all'esecuzione del contratto o trattati al solo fine di assolvere gli obblighi di legge.

L'ampliamento dell'oggetto della controprestazione del consumatore avuto riguardo al trasferimento di dati personali impone un necessario coordinamento con la disciplina ad essi relativa, ed in particolare con il Reg. (UE) 2016/679 (il "GDPR") e con i D.Lgs. 10 agosto

2018, n. 101 e 30 giugno 2003, n. 196 (il “Codice Privacy”), espressamente menzionati dall’art. 135 *novies*, co. 6, c. cons. La previsione circoscrive l’ambito di applicazione dell’intero capo sostanzialmente operando esclusioni legate a specificità settoriali e disciplinari a cui i contratti richiamati sono sottoposti (co. 2 e 3), ma ha altresì cura di stabilire che, in caso di conflitto tra norme, le disposizioni dedicate alla fornitura di contenuto digitale o di servizi digitali sono recessive rispetto a quelle contenute in altri atti dell’Unione che disciplinano uno specifico settore o oggetto (co. 5), così come rispetto a quelle del diritto dell’Unione in materia di protezione dei dati personali (co. 6).

Il ruolo sovraordinato comunque riconosciuto alla tutela dei dati personali emerge a chiare lettere dal Considerando 24 della dir. 770, che guida nell’individuare quale sia l’effettiva portata innovativa del provvedimento e, quindi, delle relative norme di recepimento. Partendo dall’osservazione della prassi, in cui «la fornitura di contenuti digitali o di servizi digitali spesso prevede che, quando non paga un prezzo, il consumatore fornisca dati personali all’operatore economico», il considerando riconosce che «la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce», ma mira ad assicurare che anche all’interno di tali modelli commerciali i consumatori non siano vittime di abusi e «abbiano diritto a rimedi contrattuali».

Più che nella legittimazione in via incidentale di un’operazione economica che coinvolge la trasmissione di dati personali a fronte della fornitura di un bene o servizio digitale, allora, la novità apportata dalla dir. 770 e dagli art. 135 *octies* ss. c. cons. sta nel riconoscere la responsabilità del professionista per la violazione dell’obbligo di conformità anche quando la relazione b2c riguarda contratti del tutto estranei allo schema della vendita perché relativi ad una «fornitura digitale», e anche qualora la corrispettività del rapporto sia data dal trasferimento di dati personali.

Salvo il caso di inadempimento totale da parte del professionista (art 135 *septiesdecies* c. cons., dedicato alla mancata fornitura), che riecheggia la previsione di cui all’art. 61 c. cons. per il caso di mancata consegna, e attribuisce al consumatore il diritto di risolvere unilateralmente il contratto ai sensi delle disposizioni successive quando il professionista «ha dichiarato, o risulta altrettanto chiaramente dalle circostanze, che non fornirà il contenuto digitale o il servizio digitale», ovvero quando sia stato convenuto o risulti che questo doveva essere fornito entro un termine essenziale, la gerarchia rimediaria prevista per la mancanza di conformità e articolata su un doppio grado di rimedi (ripristinatorio – manutentivo o distruttivo) è analoga a quella prevista dal nuovo art. 135 *bis* c. cons. Lo stesso vale per le modalità di esercizio dei rimedi di secondo ordine di cui agli artt. 135 *octiesdecies*, co. 4 – 6 e 135 *noviesdecies* c. cons.

Il modello di responsabilità del fornitore di contenuti o servizi digitali per il difetto di conformità, però, attiene ormai inevitabilmente alle modalità di esecuzione della prestazione ed è indubbio che esso consegua ad un inadempimento del professionista. Proprio in ragione dell’oggetto del contratto di fornitura di beni o servizi digitali, la valutazione di conformità si emancipa totalmente da un giudizio sulle caratteristiche effettivamente riscontrabili sul bene messo a disposizione del consumatore, e va ad incidere più ampiamente su obblighi di condotta dell’operatore economico dipendenti dalla natura del rapporto e delle prestazioni in esso dedotte. Tali obblighi, come avviene nella vendita di beni di consumo di cui al capo precedente, sono determinati in relazione a parametri soggettivi e oggettivi che ne condizionano il modo di essere conforme (art. 135 *decies* c. cons., rubricato, appunto «fornitura di contenuto digitale o servizio digitale e conformità al contratto, spec. co. 4 e 5 per i requisiti soggettivi ed oggettivi di conformità; art. 135 *undecies* c. cons., dedicato agli obblighi del professionista; art. 135 *duodecies* c. cons., relativo alla responsabilità per difetto di conformità conseguente all’errata installazione).

Anche la possibilità del professionista di modificare il contenuto digitale o il servizio digitale nei casi previsti dall'art. 135 *vicies semel* c. cons., di fatto andando ad incidere sulle modalità di esecuzione del rapporto, così come il diritto di recesso riconosciuto al consumatore ad opera del secondo comma del medesimo articolo «qualora tale modifica incida negativamente sull'utilizzo del contenuto digitale o del servizio digitale o sull'accesso allo stesso da parte del consumatore, a meno che tali conseguenze negative siano trascurabili» pare un chiaro indice in tale direzione.

Nel complesso sembra potersi dire che la tecnica legislativa prescelta e le modalità di recepimento non rivelano un'attività tesa ad assicurare un effettivo coordinamento tra le previsioni del codice del consumo, ma si limitano a testimoniare uno sforzo minimo indispensabile per conformarsi alla legislazione dell'Unione nei termini stabiliti. Rimane all'interprete il compito di ricostruire la disciplina per coglierne le potenzialità innovative e assicurarne la coerenza sistematica.

FRANCESCA BERTELLI

<https://www.gazzettaufficiale.it/eli/id/2021/11/25/21G00185/sg>  
<https://www.gazzettaufficiale.it/eli/id/2021/11/26/21G00186/sg>

2021/4(2)FP

### **Il recepimento in Germania della direttiva (UE) 2019/770.**

A partire dal gennaio 2022, i contratti di fornitura di contenuti e servizi digitali (*digitale Produkte*) saranno oggetto di una regolamentazione speciale in Germania, in attuazione della direttiva (UE) 2019/770 dell'Unione europea, di armonizzazione di alcuni aspetti del diritto contrattuale relativi alla fornitura di contenuti digitali e servizi digitali. Il Bundestag ha a tal fine approvato nel corso dell'estate una legge di modifica alla disciplina del Codice civile tedesco (25 giugno 2021, BGBl. I, p. 2123). Come noto, la summenzionata direttiva trova applicazione nei confronti di tutti i contratti in cui l'obbligo di prestazione del commerciante si riferisca ad un contenuto digitale o all'erogazione di un servizio digitale, indipendentemente dalla tipologia specifica di accordo. Siffatto approccio ha evidenziato – in Germania, così come in altri ordinamenti – il problema di giustapporre la nuova disciplina nel sistema delle regole generali del contratto. Il legislatore tedesco ha essenzialmente optato per una sua implementazione nella parte generale del BGB sull'obbligazione, dedicando una sezione apposita ai contratti relativi alla fornitura di contenuti e servizi digitali (*Verträge über digitale Produkte*, §§ 327-327u BGB). Allo stesso tempo, è stata approvata anche la legge che regola la vendita di beni con elementi digitali e altri aspetti del contratto di vendita (BGBl. I, p. 2133), che attua la direttiva (UE) 2019/771 su alcuni aspetti contrattuali della vendita di beni, anch'essa destinata ad entrare in vigore all'inizio del nuovo anno. Per la portata delle disposizioni interessate, i primi commentatori hanno paragonato la riforma sui contratti su prodotti digitali alla *Schuldrechtsmodernisierung* del 2001, riconoscendo a questi accordi negoziali natura di “*neuer Vertragstyp*”. In sintesi, il nuovo corpus di disposizioni generali prevede i) una definizione del contratto su prodotto digitale; ii) l'obbligo legale di aggiornamento del prodotto digitale; iii) la disciplina della garanzia sui prodotti digitali; iv) l'adeguamento delle disposizioni specifiche sui contratti di vendita generale, quelli di vendita al consumo, di *leasing*, di donazione, di opera e di servizio. Data la portata di armonizzazione massima prevista dalla disciplina euro-unitaria, agli Stati residuano margini invero angusti di discrezionalità nel suo

recepimento, perlopiù limitati alla determinazione dell'estensione del periodo di garanzia e delle procedure di conclusione del contratto. L'accento dell'impianto definitorio del contratto su prodotto digitale si colloca, in misura evidente, sulla determinazione del corrispettivo del contratto e, segnatamente, sul pagamento con dati personali dell'utente del servizio. Con la modifica del §312 (1) BGB e del §312 (1a) BGB, il legislatore persegue principalmente l'obiettivo di ampliare l'ambito di applicazione delle disposizioni di protezione dei consumatori (§312 BGB ss.) anche a quei contratti in cui il consumatore paga per le prestazioni del fornitore "con i suoi dati". Se finora il § 312 BGB si limitava difatti a coprire gli accordi "che hanno come oggetto una prestazione a titolo oneroso da parte del commerciante", le nuove disposizioni si riferiscono più genericamente all'impegno del consumatore di "pagare un prezzo", che può anche consistere nel "fornire al commerciante o nell'impegnarsi a fornirgli dati personali" (§ 312, 1a BGB). Secondo il memorandum di accompagnamento alla legge di riforma, non assume rilievo la circostanza per cui il consumatore fornisca attivamente i dati al commerciante o se il commerciante usi o elabori in altro modo i dati già a sua disposizione per ragioni diverse. Tuttavia, il §312 (1a), frase 2 BGB esclude l'applicazione di questo apparato di disposizioni quando il professionista "tratti i dati personali forniti dal consumatore esclusivamente al fine di adempiere ai suoi obblighi di prestazione o ai requisiti legali impostigli e non li tratta per qualsiasi altro scopo". Pertanto, se un professionista elabora, per esempio, i dati dell'indirizzo del consumatore per inviargli i beni ordinati, o se memorizza i dati di fatturazione per scopi contabili e fiscali, questo non comporta l'applicabilità delle disposizioni relative di protezione dei consumatori. La situazione ovviamente cambia qualora il professionista elabori anche l'indirizzo o i dati di fatturazione per altri scopi, ad esempio per proporre pubblicità mirate al singolo consumatore. Nei riguardi della determinazione del prezzo – oltre alla possibilità che il corrispettivo sia costituito dal pagamento con dati personali –, il § 327(1) BGB include inoltre ogni rappresentazione digitale di un valore, quale l'erogazione di buoni, *coupon*, *tokens* elettronici, *cryptovalute* etc. La prestazione principale in capo al professionista è quella relativa all'obbligo di fornitura del contenuto o servizio digitale (§ 327b BGB). Salvo diversa previsione contrattuale, il consumatore può richiedere la prestazione immediatamente dopo la conclusione del contratto, ossia non appena il contenuto digitale o il mezzo appropriato per accedere o scaricare il contenuto digitale è stato messo a disposizione o reso accessibile al consumatore direttamente, ovvero tramite un dispositivo designato dal consumatore a tale scopo (§327b (3) BGB). Il codice chiarisce inoltre che "mettere a disposizione" significa che il consumatore viene dotato di un accesso indipendente che gli consenta di impiegare un servizio sotto il controllo di terzi, non rilevando che il servizio sia effettivamente utilizzato. Un'innovazione di particolare rilievo è quella relativa all'obbligo del fornitore del prodotto digitale di assicurare gli aggiornamenti (compresi quelli di sicurezza) necessari per mantenere la conformità contrattuale del prodotto digitale entro un dato lasso di tempo (§ 327f (1) BGB). Rispetto alla portata dell'obbligo, occorre comunque notare come il riferimento alla "conformità contrattuale del prodotto digitale" non copra la fornitura di aggiornamenti che determinino un miglioramento funzionale del prodotto, quali, ad esempio, il rilascio di software che rendano compatibile una smart TV con applicazioni sviluppate dopo la sua messa in commercio. Il periodo in cui debba essere assicurata la messa a disposizione di aggiornamenti varia in relazione alle caratteristiche del contratto: nel caso di un contratto per la fornitura permanente di un prodotto digitale, il periodo rilevante è quello concordato di fornitura (§ 327c(1) frase 3 n. 1 BGB); in tutti gli altri casi, il periodo rilevante è quello che il consumatore può ragionevolmente aspettarsi in base alla natura e allo scopo del prodotto digitale e tenendo conto delle circostanze e della natura del contratto. Ad ogni modo, se pur non chiarendo del tutto cosa debba intendersi per "aspettativa ragionevole", il memorandum di accompagnamento precisa che l'obbligo di aggiornamento non debba necessariamente

limitarsi al relativo periodo di garanzia. In particolare, il legislatore tedesco ritiene che possa distinguersi tra sistema operativo e software applicativo. Così, un sistema operativo per un dispositivo che richieda l'accesso a Internet dovrebbe essere fornito di aggiornamenti per un periodo di tempo più lungo a causa della sua importanza centrale rispetto al *software* applicativo il cui uso non richieda l'utilizzo di una connessione. La disciplina sui contratti a contenuto digitale introduce una significativa deroga a quella generale sulla vendita anche in punto di rimedi in caso di difformità del prodotto. In primo luogo, il consumatore ha diritto alla rimozione dei difetti, entro un tempo ragionevole dalla comunicazione e senza notevoli inconvenienti per il consumatore (§ 327l BGB). Contrariamente al diritto generale di vendita, però, il consumatore non ha il diritto di scegliere se vuole che il prodotto digitale sia riparato o reso nuovamente disponibile, sempre che questo sia ragionevolmente possibile. Questa decisione spetta piuttosto al professionista, vale a dire quella se voglia rimediare al difetto inviando una versione aggiornata del prodotto digitale o mettendo nuovamente a disposizione una copia priva di difetti. Quando la rimozione dei difetti sia impossibile o eccessivamente gravosa per il professionista, il consumatore ha diritto a risolvere il rapporto attraverso una corrispondente comunicazione al professionista (§ 327l (2) BGB). In linea di massima, il consumatore può risolvere il contratto solo se il prodotto digitale ha un difetto che non è irrilevante (§ 327m (2) BGB). Tuttavia, questo limite non si applica se si tratta di un contratto per la fornitura di contenuti digitali e servizi digitali in cui il consumatore fornisce o si è impegnato a fornire dati personali. Tali contratti possono difatti essere risolti dal consumatore anche nel caso di un difetto di minor rilevanza, data la maggior tutela da assicurarsi al valore del dato personale quale moneta di scambio. Qualora non intenda chiedere la risoluzione, il consumatore può comunque domandare la riduzione del prezzo (§327n (1) frase 1 BGB). In caso di risoluzione del contratto, il professionista deve rimborsare al consumatore i pagamenti effettuati per adempiere al contratto e gli è fatto divieto di far uso del contenuto che il consumatore abbia fornito o creato quando ha usato il prodotto digitale fornito dal commerciante dopo la fine del contratto (§327p (2) frase 1 BGB). Nella misura in cui tali contenuti contengono dati personali, non troveranno tuttavia applicazione le disposizioni del Titolo del BGB sui contratti a contenuto digitale, quanto quelle del GDPR (che consente, a talune condizioni, il diritto del consumatore alla cancellazione del dato personale). Infine, alcune rilevanti previsioni sono dedicate alla possibilità per il fornitore di modificare in via unilaterale le caratteristiche del prodotto digitale. La legge tedesca permette queste modifiche, alle condizioni stabilite al § 327r (1) BGB, ossia che i) il contratto preveda espressamente questa possibilità, ii) ci sia un motivo valido, iii) il consumatore non sostenga costi aggiuntivi e iv) sia informato in modo chiaro e comprensibile. Il Considerando 75 della direttiva (UE) 2019/770 cita a titolo esemplificativo, i cambiamenti necessari per adattare il prodotto digitale a un nuovo ambiente tecnico o all'aumento del numero di utenti. Inoltre, se la capacità del consumatore di accedere al prodotto digitale o l'usabilità del prodotto digitale per il consumatore è compromessa nel corso della modifica del prodotto digitale, essa può essere fatta solo se il consumatore è sufficientemente informato entro un periodo di tempo ragionevole su un supporto durevole sulle caratteristiche e il tempo della modifica così come i suoi diritti legali, quali il diritto di risolvere il rapporto (salvo che il prodotto conservi la sua utilizzabilità senza costi aggiuntivi) (§ 327r BGB).

FEDERICO PISTELLI

<https://dejure.org/BGBI/2021/BGBI. I S. 2123>

2021/4(3)CR

**Le rilevanti modifiche al Codice Privacy introdotte dal ‘Decreto Capienze’ del 7 ottobre 2021 come convertito in legge con modifiche ad opera della legge 3 dicembre 2021 n. 205.**

Il 7 ottobre 2021 è stato approvato dal Consiglio dei Ministri, e pubblicato in Gazzetta Ufficiale il giorno successivo, il decreto-legge n. 139/2021 (“**Decreto Capienze**”) con il dichiarato obiettivo di prevedere degli allentamenti alle misure anti-Covid introdotte nei mesi precedenti. Nell’ambito di tale intervento il Governo ha inteso disciplinare anche alcuni aspetti in materia di protezione dei dati personali: l’art. 9 del Decreto Capienze, infatti, ha introdotto significative modifiche al D.Lgs. 196/2003 (“**Codice Privacy**”) volte a snellire e semplificare l’attività della Pubblica Amministrazione, ma che hanno fatto molto discutere proprio per il significativo ampliamento dei poteri della Pubblica Amministrazione in materia di protezione dei dati personali e per la corrispondente riduzione dei poteri di controllo e vigilanza dell’Autorità garante per la protezione dei dati personali (“**Garante Privacy**”). Tali modifiche sono state in gran parte confermate e, anzi, ampliate dalla legge 3 dicembre 2021, n. 205 che ha convertito con modificazioni il Decreto Capienze (la “**legge di conversione**”).

Un primo intervento riguarda la semplificazione nell’utilizzo delle basi giuridiche del trattamento. Il comma 1 dell’art. 9 come previsto dalla legge di conversione modifica l’art. 2-ter del Codice Privacy prevedendo che la base giuridica di cui all’art. 6, para. 3, lett. b) del GDPR può essere costituita non più solamente da una norma di legge o di regolamento, ma anche da “*atti amministrativi generali*”. La norma, inoltre, introduce un nuovo comma 1-bis del Codice Privacy ai sensi del quale il trattamento da parte di un’autorità pubblica può essere consentito anche “*se necessario per l’adempimento di un compito svolto nel pubblico interesse o per l’esercizio di pubblici poteri a essa attribuiti*”. Questo significa che di fatto la Pubblica Amministrazione potrà sempre trattare dati personali ogni qual volta lo ritenga necessario per lo svolgimento delle proprie funzioni, ponendo come fondamento di tale trattamento un mero atto amministrativo.

Altra importante novità, non presente nel Decreto Capienze e introdotta in sede di conversione, riguarda la comunicazione e la diffusione di dati personali. L’art. 2-ter del Codice Privacy prevedeva che la comunicazione di dati personali fra titolari di trattamenti effettuati per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri fosse consentita solo in presenza di una norma di legge (o di regolamento) e, in assenza di tale norma, era necessario effettuare una comunicazione al Garante che aveva 45 giorni di tempo per indicare le misure da adottare a garanzia degli interessati. La diffusione era invece possibile solo in presenza di una norma di legge o di regolamento. Il nuovo art. 2-ter prevede invece che sia la comunicazione che la diffusione saranno consentite non solo se previste da una norma di legge o di regolamento, ma anche se necessarie ai sensi del comma 1-bis (cioè se necessarie per l’adempimento di un compito svolto nel pubblico interesse o per l’esercizio di pubblici poteri), con l’unico vincolo di doverne dare notizia al Garante almeno dieci giorni prima dell’inizio della comunicazione o diffusione.

La legge di conversione è intervenuta anche sul trattamento di categorie particolari di dati personali per motivi di interesse pubblico rilevante. L’art. 2-sexies del Codice Privacy, modificato dalla legge 205/2021, prevede infatti che anche i trattamenti delle categorie particolari di dati personali di cui all’art. 9 GDPR potranno essere previsti, oltre che da norme di legge e di regolamento, da “*atti amministrativi generali*”. Per i dati personali relativi alla salute che siano “*privi di elementi identificativi diretti*” viene introdotta dal nuovo comma 1-bis dell’art.

2-*sexies* una disciplina specifica che prevede la definizione delle modalità e delle finalità del trattamento con decreto del Ministro della salute previo parere del Garante.

In sede di conversione è stata confermata la scelta, particolarmente criticata, di abrogare per intero l'art. 2-*quinquiesdecies* del Codice Privacy che prevedeva la possibilità di un controllo preventivo da parte del Garante sui trattamenti ad alto rischio svolti per l'esecuzione di un compito di interesse pubblico, con la facoltà per l'Autorità di imporre l'adozione di misure a tutela degli interessati. Tale modifica fa venire meno un importante strumento di tutela preventiva degli interessati di cui il Garante si è più volte avvalso per evitare che alcune misure adottate dal Governo, anche nell'ambito della lotta al Covid-19 (ad esempio con riferimento all'App IO e al *Green pass*), potessero risultare in una limitazione dei diritti e delle libertà degli individui.

In un'ottica analoga si colloca il comma 7 dell'art. 9 della legge di conversione che stabilisce un termine perentorio di 30 giorni entro cui l'Autorità potrà pronunciarsi su riforme, misure e progetti del Piano nazionale di ripresa e resilienza (PNRR). Decorso tale termine il Governo potrà andare avanti senza più la necessità di acquisire il parere.

La legge di conversione ha invece eliminato la norma del Decreto Capienze che, in tema di dati di traffico, abrogava il comma 5 dell'art. 132 del Codice Privacy che attribuisce al Garante il potere di prescrivere misure a tutela degli interessati con riferimento a trattamenti finalizzati alla prevenzione di reati e di stabilire le modalità per la distruzione delle informazioni entro due anni nel caso del traffico telefonico, ed entro un anno per il traffico telematico.

Il Decreto Capienze è poi intervenuto sul reato di diffusione illecita di immagini o video sessualmente espliciti (c.d. *revenge porn*) di cui all'art. 612-*ter* c.p. Questo intervento è stato confermato e rafforzato dalla legge di conversione che ha aggiunto al Codice Privacy l'art. 144-*bis* secondo cui “*chiunque, inclusi i minori ultraquattordicenni, abbia fondato motivo di ritenere che le registrazioni audio, immagini o video o altri documenti informatici a contenuto sessualmente esplicito che lo riguardano, destinati a rimanere privati, possano essere oggetto di invio, consegna, cessione, pubblicazione o diffusione attraverso piattaforme digitali senza il suo consenso ha facoltà di segnalare il pericolo al Garante*”. Nel caso di minori, la segnalazione al Garante può essere fatta anche da chi esercita la responsabilità genitoriale o la tutela. Il Garante è tenuto a provvedere entro 48 ore dalla segnalazione e può adottare provvedimenti nei confronti dei gestori delle piattaforme digitali anche indicando le misure per la conservazione a fini probatori del materiale oggetto della segnalazione.

Un ulteriore rilevante intervento, non presente del Decreto Capienze e introdotto con la legge di conversione, riguarda la c.d. moratoria per i sistemi di videosorveglianza con sistemi di riconoscimento facciale. Il comma 9 dell'art. 9 della legge di conversione prevede infatti la sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale attraverso dati biometrici, in luogo pubblico o aperto al pubblico, da parte di soggetti sia pubblici che privati, fino a che non sarà adottata una disciplina specifica, e comunque non oltre il 31 dicembre 2023. Tuttavia, la portata di tale sospensione viene ridotta dal successivo comma 12 che ne esclude l'applicabilità ai trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati. In questi casi, pertanto, l'utilizzo degli impianti di videosorveglianza con sistemi di riconoscimento facciale sembra essere già consentito previo parere del Garante, parere comunque non necessario se si tratta di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali o di quelle giudiziarie del pubblico ministero.

Dall'esame delle modifiche sopra riportate si può concludere che la legge di conversione ha realizzato una profonda modifica del Codice Privacy, andando ben al di là della situazione emergenziale legata al Covid-19. In particolare, se da un lato ha ampliato i compiti del

Garante con riferimento al *revenge porn*, dall'altro ne ha significativamente ridotto i poteri di controllo e vigilanza nei confronti della Pubblica Amministrazione, la quale si trova ora di fatto a poter decidere in sostanziale autonomia quali dati trattare, a chi comunicarli, e se diffonderli. Il rischio è di scalfire le tutele previste in favore degli interessati esponendoli al pericolo di lesione dei loro diritti e libertà fondamentali, nonché di far emergere l'idea che la protezione dei dati personali rappresenti un ostacolo all'attività dei soggetti pubblici e che, come tale, possa essere sacrificata in nome di altri interessi considerati prevalenti.

CHIARA RAUCCIO

<https://www.gazzettaufficiale.it/eli/id/2021/10/08/21G00153/sg>  
<https://www.gazzettaufficiale.it/eli/id/2021/12/07/21G00228/sg>

2021/4(4)RA

**Verso il Data Governance Act: le modifiche del Consiglio dell'Unione Europea del 24 settembre 2021 alla proposta di regolamento della Commissione, approvate dal Comitato dei rappresentanti permanenti il 1 ottobre 2021 con contestuale mandato alla Presidenza del Consiglio di avviare le negoziazioni con il Parlamento Europeo.**

Come noto, nel corso dell'ultimo decennio l'ingresso nel mercato di tecnologie *disruptive*, capaci di influenzare ogni settore dell'economia e della vita quotidiana, è stato accompagnato da un (sempre maggiore) utilizzo dei dati, i quali sono divenuti – in definitiva – un essenziale fattore economico trainante.

I dati rappresentano, dunque, il fulcro delle trasformazioni tecnologiche digitali cui stiamo assistendo e l'Unione Europea – che aspira a divenire *leader* di una società basata sui dati – ha adottato una propria 'strategia', con la quale essa intende dar vita a uno 'spazio comune europeo di dati'.

Nell'ambito di tale 'strategia per i dati', il 25 novembre 2020, la Commissione Europea ha adottato una proposta di regolamento relativo alla *governance* europea dei dati (“**Atto sulla governance dei dati**” o “**Data Governance Act**” o “**DGA**”).

Tale proposta, volta a promuovere la disponibilità dei dati utilizzabili tramite il rafforzamento della fiducia negli intermediari di dati e il potenziamento dei meccanismi di condivisione dei dati in tutta l'Unione Europea, si prefigge di affrontare quattro fondamentali questioni: (i) la messa a disposizione dei dati del settore pubblico per il 'riutilizzo', qualora tali dati siano oggetto di diritti di terzi; (ii) la condivisione dei dati tra le imprese, dietro compenso in qualsiasi forma; (iii) il consenso all'utilizzo di dati personali con l'aiuto di un intermediario; e (iv) il consenso all'utilizzo dei dati per scopi altruistici.

Alla luce di tali obiettivi, l'iniziativa della Commissione va a intersecarsi con la vigente legislazione europea in materia di dati personali, all'interno della quale, come noto, godono di enorme rilevanza il Regolamento Generale sulla Protezione dei Dati (il “**GDPR**”) e la direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche (la “**Direttiva ePrivacy**”), nonché la direttiva (UE) 2019/1024 del Parlamento Europeo e del Consiglio del 20 giugno 2019 (la così detta “**Open Data Directive**”), che il *Data Governance Act* si prefigge di affiancare per integrare la disciplina del settore pubblico. Invero, l'*Open Data Directive* – che stabilisce il quadro giuridico per il riutilizzo delle informazioni e dei dati del settore pubblico – espressamente esclude dal proprio ambito di applicazione le sorti dei

dati oggetto di diritti di terzi detenuti da enti pubblici (art. 1.2 lett. c) *Open Data Directive*), la cui disciplina rientra, invece, negli scopi del DGA.

Lo scorso 24 settembre 2021, il Consiglio dell'Unione Europea ha adottato – in sede di prima lettura – alcune modifiche alla proposta della Commissione, con l'obiettivo di meglio definire la relazione tra DGA e GDPR, nonché di chiarire e meglio definire in un nuovo documento, le misure già prospettate dalla Commissione, invitando contestualmente il Comitato dei rappresentanti permanenti del Consiglio (Coreper) ad approvare il documento in guisa di mandato per la Presidenza ad avviare negoziati con il Parlamento Europeo. L'approvazione del testo da parte del Coreper, avvenuta lo scorso 1 ottobre 2021, permetterà dunque alla Presidenza del Consiglio di avviare tali negoziati con il Parlamento Europeo. Sia il Consiglio che il Parlamento Europeo dovranno, poi, approvare il testo definitivo.

Procedendo a illustrare i contenuti della proposta, così come modificata dal Consiglio dell'UE, è bene principiare dal **Capo I**, il quale si occupa di definire l'oggetto e l'ambito di applicazione dell'Atto sulla *governance* dei dati.

In particolare, l'art. 1 del DGA prevede che il regolamento si occupi di stabilire, senza alterare gli obblighi e i diritti racchiusi nel GDPR: *a)* le condizioni per il 'riutilizzo' di determinate categorie di dati detenuti da enti pubblici; *b)* un quadro di notifica e vigilanza 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.

L'art. 2 precisa poi, *inter alia*, le definizioni di:

- 'riutilizzo', per tale intendendosi "*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. 2.2);

- 'servizio di intermediazione dei dati', ovvero sia "*un servizio commerciale, il quale ha come obiettivo principale quello di stabilire relazioni giuridiche o commerciali dirette ai fini della condivisione dei dati, mediante mezzi tecnici, giuridici o di altro tipo, tra un numero indefinito di interessati e di titolari dei dati, da un lato, e di utenti dei dati dall'altro, in particolare per l'esercizio dei diritti degli interessati in relazione ai dati personali*"; categoria dalla quale vanno espressamente esclusi i "*servizi che ottengono dati dai titolari dei dati, li aggregano, li arricchiscono o li trasformano e concedono in licenza agli utenti l'uso dei dati risultanti, senza stabilire una relazione diretta tra i titolari e gli utenti dei dati*", i "*servizi che si concentrano sull'intermediazione di contenuti, in particolare di contenuti protetti dal diritto d'autore*", "*i servizi di piattaforme di scambio di dati utilizzati esclusivamente da un titolare dei dati per consentire l'uso dei dati in suo possesso, nonché le piattaforme sviluppate e offerte esclusivamente dai produttori di oggetti e dispositivi collegati all'Internet delle Cose, il cui obiettivo principale è garantire le funzionalità dell'oggetto o del dispositivo collegato e consentire servizi a valore aggiunto*" e gli "*organismi del settore pubblico che offrono strutture di intermediazione per la condivisione dei dati su base non commerciale*" (art. 2.2a);

- 'altruismo dei dati', che indica "*la volontaria condivisione dei dati da parte degli interessati o dei titolari dei dati senza cercare una ricompensa, per obiettivi di interesse generale definiti in conformità con il diritto nazionale, ove applicabile, come ad esempio scopi di ricerca scientifica, elaborazione di politiche o miglioramento dei servizi pubblici*" (art. 2.10).

Il **Capo II** del DGA si occupa, invece, di istituire un meccanismo idoneo a consentire il riutilizzo di determinate categorie di dati protetti detenuti da enti pubblici, subordinato al rispetto dei diritti dei terzi (fra cui, ad esempio, i diritti di proprietà intellettuale, il *trade secret* e la protezione dei dati personali). L'art. 3.3 sottolinea, in particolare, che le disposizioni del Capo in parola non danno vita ad alcun obbligo in capo agli enti pubblici di consentire il

riutilizzo dei dati né esentano i medesimi enti dai loro obblighi di riservatezza. Esse sono, piuttosto, volte a porre in essere una serie di condizioni basilari idonee a consentire il riutilizzo dei dati (cfr. art. 5 – condizioni che debbono essere non discriminatorie, proporzionate e oggettivamente giustificate in relazione alle finalità del riutilizzo e alle categorie e alla natura dei dati), qualora tale facoltà venga concessa dall’ente pubblico (anche dietro pagamento di una “*tariffa*” – cfr. art. 6).

Ancora, al Capo II viene introdotta la necessità per gli Stati Membri di introdurre un “*punto di contatto unico*” a sostegno dei ricercatori e delle imprese innovative per l’identificazione dei dati idonei, nonché alcune strutture volte a sostenere gli enti pubblici con mezzi di assistenza tecnica e giudiziaria.

L’art. 8a, introdotto dal Consiglio, prevede poi che – a meno che le leggi dei singoli Stati Membri dispongano un termine inferiore – le decisioni sul riutilizzo debbono avvenire entro due mesi dalla data di ricezione della richiesta (salvo possibilità di prorogare, in casi eccezionali, il termine per ulteriori 30 giorni). Il medesimo articolo garantisce, inoltre, a ogni persona fisica o giuridica direttamente interessata da tali decisioni un diritto di ricorso avverso le medesime, la cui effettiva applicazione sarà regolata dalla legge nazionale di ciascuno Stato Membro.

Il **Capo III** rivolge, invece, l’attenzione ai requisiti applicabili ai servizi di intermediazione dei dati. In particolare, le disposizioni in esso contenute mirano ad accrescere la fiducia nella condivisione dei dati (personali e non), come pure a ridurre i costi di transazione relativi alla condivisione dei dati tra imprese (B2B) e da consumatore a impresa (C2B), grazie alla creazione di un regime di notifica per i fornitori di servizi di intermediazione dei dati.

Invero, l’art. 9 del DGA prevede che la fornitura di servizi di intermediazione dei dati (individuati dal medesimo articolo nella “*intermediazione tra le persone giuridiche titolari dei dati e i potenziali utenti*”, nella “*intermediazione tra interessati che intendono mettere a disposizione i propri dati personali e potenziali utenti dei dati*” e nei “*servizi di cooperative di dati*”) sia soggetta al rispetto delle condizioni previste dall’art. 11, nonché al rispetto di una peculiare procedura di notifica disciplinata all’art. 10 del DGA.

Quest’ultima disposizione stabilisce che i fornitori di servizi di intermediazione dei dati – anche qualora siano stabiliti fuori dal territorio UE (nel qual caso, sono tenuti a nominare un legale rappresentante in uno Stato Membro) – che intendano fornire i servizi di cui all’art. 9 del DGA devono presentare una notifica all’Autorità competente designata dallo Stato Membro (e comunicata alla Commissione). Una volta presentata la notifica, che deve contenere le informazioni specificamente previste dal medesimo art. 9, i fornitori possono iniziare la loro attività, tenuto conto che l’Autorità competente dovrà tenere un registro dei fornitori di servizi di intermediazione dei dati all’interno dell’Unione. Qualora, poi, uno dei fornitori cessasse le proprie attività dovrà darne notizia all’Autorità competente, la quale provvederà a informare la Commissione.

L’art. 11 del DGA, come accennato, prevede poi una serie di condizioni da rispettare nella fornitura di servizi di intermediazione dei dati, tra le quali rilevano in particolare: 1) il divieto di utilizzare i dati per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati e la necessità di fornire i servizi di intermediazione dei dati mediante un’entità giuridica distinta; 2) l’utilizzo dei dati raccolti nel corso della fornitura del servizio solo per lo sviluppo di tale servizio; 3) l’agevolazione dello scambio dei dati mediante la conversione in formati specifici, allo scopo di migliorare l’interoperabilità a livello intrasettoriale e intersettoriale; 4) la possibilità di offrire servizi aggiuntivi volti a facilitare lo scambio di dati quali l’archiviazione, la cura, la pseudonimizzazione e l’anonimizzazione dei dati; 5) la previsione di una procedura di accesso al servizio che sia equa, trasparente e non discriminatoria, anche per quanto riguarda i prezzi; 6) la previsione di procedure per prevenire pratiche fraudolente o abusive

in relazione all'accesso ai dati da parte di soggetti che richiedono l'accesso tramite i suoi servizi; 7) la garanzia di una ragionevole continuità nella fornitura dei servizi; 8) l'adozione di misure ragionevoli volte ad assicurare l'interoperabilità con altri servizi di intermediazione dei dati; 9) l'adozione di adeguate misure tecniche, giuridiche e organizzative volte a prevenire l'illegittimo trasferimento o accesso a dati non personali; 10) l'informare, senza ritardo, gli interessati in caso di trasferimento, accesso o utilizzo non autorizzato di dati non personali che ha condiviso; 11) il mantenimento di un appropriato livello di sicurezza per l'archiviazione e la trasmissione dei dati non personali; 12) la facilitazione dell'esercizio dei diritti degli interessati; 13) la specificazione della giurisdizione o delle giurisdizioni al di fuori dell'UE in cui si intende effettuare l'utilizzo dei dati e la indicazione agli interessati degli strumenti necessari per fornire o ritirare il loro consenso al trattamento; 14) la conservazione di un registro delle attività di intermediazione.

Sull'osservanza di tali condizioni vigila l'Autorità competente individuata da ciascuno Stato Membro, la quale si occupa altresì del monitoraggio e della supervisione del rispetto della normativa da parte dei servizi di intermediazione dei dati qualora venga richiesto da parte di persone fisiche o giuridiche (art. 13.1). L'Autorità competente ha anche il potere di richiedere ai fornitori le informazioni necessarie per verificare la conformità ai requisiti previsti dal Capo III e, qualora ne constati l'inosservanza, informa il fornitore, consentendogli di esprimere le proprie osservazioni entro 30 giorni (art. 13.3). L'Autorità ha poi il potere di ordinare la cessazione della violazione e di imporre sanzioni pecuniarie dissuasive nei confronti dei trasgressori (art. 13.4).

Sempre con riguardo al Capo III, va infine osservato che le disposizioni ivi contenute 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 (art. 14).

All'altruismo dei dati è dedicato il **Capo IV**, 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 DGA – che lascia notevole spazio all'autonomia organizzativa e tecnica dei singoli Stati Membri (cfr. art. 14a) – consente ai soggetti interessati di chiedere di essere iscritti a un “*registro nazionale delle organizzazioni per l'altruismo dei dati riconosciute*” (art. 15), che sarà tenuto a cura dell'Autorità competente designata da ciascuno Stato Membro (art. 20). Le organizzazioni registrate, in possesso dei requisiti di cui all'art. 16 del DGA, saranno riconosciute in tutta l'Unione Europea, creando così la necessaria fiducia nell'altruismo dei dati e incoraggiando 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 alle organizzazioni per l'altruismo dei dati riconosciute emerge, in particolare, l'adesione a un codice di condotta adottato dalla Commissione in collaborazione con gli *stakeholders* (artt. 16.d e 19).

Il **Capo V** del DGA stabilisce i requisiti per il funzionamento delle Autorità competenti dei singoli Stati Membri, incaricate del monitoraggio e dell'attuazione del quadro di notifica per i fornitori di servizi di intermediazione dei dati e per gli enti che praticano l'altruismo dei dati, di cui agli articoli 12 e 20. Il Capo V contiene, inoltre, alcune disposizioni volte a disciplinare il diritto dei consociati di presentare reclami contro le decisioni di tali enti e fornitori, nonché i mezzi di ricorso giurisdizionale, in relazione alle materie che ricadono nell'ambito di applicazione del medesimo DGA.

Il **Capo VI** istituisce poi un gruppo di esperti, denominato “*Comitato Europeo per l'innovazione in materia di dati*”, con l'obiettivo, fra l'altro, di consigliare e assistere la

Commissione nel rafforzare l'interoperabilità dei servizi di intermediazione dei dati e garantire una prassi coerente nel trattamento delle richieste di dati detenuti da enti pubblici.

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

Infine, il **Capo VIII** del DGA contiene una serie di disposizioni transitorie e finali volte a proteggere dall'accesso e dal trasferimento internazionale illecito i dati detenuti da enti pubblici, da servizi di intermediazione dei dati e da organizzazioni per l'altruismo dei dati.

L'applicazione delle norme racchiuse nel DGA – che non dovrà incidere sull'applicazione delle disposizioni vigenti in materia di concorrenza e, in particolare, sull'applicazione degli articoli 101 e 102 del trattato sul funzionamento dell'Unione Europea (“TFUE”) con riguardo allo scambio di informazioni sensibili dal punto di vista della concorrenza attraverso servizi di intermediazione dei dati tra concorrenti effettivi o potenziali – è prevista a decorrere dal 18° mese successivo alla entrata in vigore del *Data Governance Act* medesimo (art. 35).

Al fine, poi, di scongiurare il rischio di obsolescenza normativa, sempre insito in simili iniziative, ai sensi dell'art. 32 del DGA, la Commissione dovrà effettuare una valutazione circa l'applicazione dell'Atto sulla governance dei dati e presentare al Parlamento Europeo, al Consiglio e al Comitato economico e sociale una relazione sulle principali conclusioni tratte, entro 48 mesi dal termine indicato al menzionato art. 35.

RICCARDO ALFONSI

<https://data.consilium.europa.eu/doc/document/ST-12124-2021-INIT/en/pdf>

2021/4(5)EMI

### **La sentenza della Corte di Giustizia UE del 6 ottobre 2021 sul diritto di decompilazione del software (il caso Top System)**

Il 6 ottobre 2021 la Quinta Sezione della Corte di Giustizia dell'Unione Europea si è pronunciata sulla domanda di rinvio pregiudiziale promossa dalla *Cour d'appel de Bruxelles*, nell'ambito del procedimento *Top System SA vs. État belge* (C-13/20), avente ad oggetto l'interpretazione dell'articolo 5, paragrafo 1, della direttiva 91/250/CEE del Consiglio, del 14 maggio 1991, relativa alla tutela giuridica dei programmi per elaboratore.

La controversia vede contrapporsi, da un lato, *Top System SA*, società di diritto belga che sviluppa programmi per elaboratore e fornisce prestazioni di servizi informatici e, dall'altro, *Selor*, l'ente pubblico belga responsabile della selezione e dell'orientamento dei collaboratori della pubblica amministrazione. Su richiesta di *Selor*, *Top System* aveva sviluppato diverse specifiche applicazioni. Il 6 febbraio 2008 *Selor* e *Top System* avevano concluso un contratto avente ad oggetto l'installazione e la configurazione di un nuovo ambiente informatico di produzione, che, però, presentava dei difetti di funzionamento. Si noti che *Selor* detiene una licenza d'uso su tutti i programmi appositamente creati da *Top System*.

Il 6 luglio 2009 la *Top System* ha proposto ricorso contro *Selor* e lo Stato belga dinanzi al *Tribunal de commerce de Bruxelles*, contestando l'illegittima attività di decompilazione effettuata da *Selor* sul programma per elaboratore e richiedendo il risarcimento dei danni per la decompilazione così effettuata.

Il 26 novembre 2009 la causa è stata rinviata dinanzi al *Tribunal de première instance de Bruxelles* che, il 19 marzo 2013, ha dichiarato la domanda così proposta come infondata.

La *Top System* ha, quindi, impugnato la sentenza di primo grado dinanzi al giudice del rinvio, la *Cour d'appel de Bruxelles*, sostenendo che la decompilazione può essere effettuata solo in forza di un'autorizzazione dell'autore, o del suo avente diritto, o ancora a fini della c.d. interoperabilità - ovvero, l'interconnessione e l'interazione funzionale tra software.

Per contro, sulla base dell'interpretazione dell'art. 6 della Legge del 30 giugno 1994, che ha recepito nell'ordinamento belga la direttiva 91/250/CEE, *Selor* riteneva di essere legittimato a procedere alla decompilazione per correggere alcuni errori di funzionamento che rendevano impossibile un uso conforme alla destinazione del *software* e ad osservare, studiare e sperimentare il funzionamento del programma allo scopo di determinare le idee alla base delle funzionalità con l'obiettivo di prevenire le future interruzioni determinate da simili errori.

Alla luce dei presenti elementi di fatto ed avendo accertato l'avvenuta decompilazione da parte di *Selor*, la Corte d'Appello Belga proponeva, quindi, due differenti questioni pregiudiziali all'attenzione della Corte di Giustizia.

In merito alla prima questione, ci si domanda se l'articolo 5, paragrafo 1, della direttiva 91/250 ("Deroghe relative alle attività riservate") debba essere interpretato nel senso che il legittimo acquirente di un programma per elaboratore ha il diritto di procedere alla decompilazione di tutto o parte di esso al fine di correggere errori che incidono sul funzionamento di tale programma, anche quando la correzione consista nel disattivare una funzione che pregiudica il buon funzionamento dell'applicazione di cui fa parte detto programma.

A tal riguardo, la Corte ricorda che la decompilazione di un software è una attività di *reverse engineering* che consiste nella ricostruzione del codice sorgente partendo da un codice oggetto di un programma esistente. Attraverso la decompilazione, di regola, si ottiene un "quasi codice sorgente", non perfettamente corrispondente al codice sorgente originale. L'attività di *reverse engineering* rappresenta il contraltare, in ambito *software*, della c.d. compilazione, attività che attiene, invece, al processo di creazione del codice oggetto sulla base delle istruzioni contenute nel codice sorgente.

Siccome la decompilazione non è testualmente ricompresa tra gli atti disciplinati dall'art. 4 lett. a) e b) della direttiva, ai quali fa riferimento l'art. 5 par. 1, la Corte, nelle sue ricostruzioni, pone l'interrogativo sulla possibilità di estendere tale disciplina anche agli atti di decompilazione. A tal riguardo, la Corte sostiene che il legittimo acquirente di un programma non solo ha il diritto di decompilazione ai fini di interoperabilità a norma dell'art. 6 della direttiva, ma ha anche il diritto di decompilazione nel caso in cui ciò sia necessario per risolvere errori che incidono sul buon funzionamento del software, come previsto dall'art. 5, par. 1.

In merito, invece, alla seconda questione (ovvero, se il legittimo acquirente di un programma per elaboratore che intenda procedere alla decompilazione al fine di correggere gli errori che incidono sul suo funzionamento debba soddisfare i requisiti previsti all'articolo 6 della direttiva), la Corte chiarisce i confini ed i presupposti dell'attività di decompilazione *ex art. 5*.

La decompilazione, infatti, deve essere necessaria per la correzione di errori e per consentire al legittimo acquirente un uso conforme alla destinazione del programma; la rettifica degli errori secondo il modello dell'art. 5 deve rispettare le specifiche previsioni contrattuali che non possono in ogni modo vietare simili atti di correzione; il legittimo acquirente non può utilizzare il risultato della decompilazione per fini diversi dalla correzione di errori di funzionamento.

Pertanto, come si legge nella sentenza, il legittimo acquirente che intenda procedere alla decompilazione al fine di correggere errori di funzionamento del software potrà agire

soltanto nella misura necessaria a tale correzione e nel rispetto, se del caso, delle condizioni contrattualmente previste con il titolare del diritto d'autore su detto programma, non dovendo, però rispettare i requisiti dettati dall'art. 6 della direttiva.

La sentenza in esame non solo presenta interessanti spunti di indagine circa l'ambito applicativo della tutela autoriale dei *software* ma impone anche necessarie riflessioni in merito alle nuove possibili frontiere di tutela dei programmi per elaboratore.

ENZO MARIA INCUTTI

<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62020CJ0013&from=it>

2021/4(6)FG

### **La sentenza della *Court of Appeal* del 21 settembre sul caso Dabus: l'intelligenza artificiale può essere considerata inventore?**

Con sentenza del 21 settembre 2021 (*Thaler v Comptroller General of Patents Trade Marks and Designs* [2021] EWCA Civ 1374), la *Court of Appeal* del Regno Unito ha stabilito che un sistema di intelligenza artificiale non può qualificarsi come “inventore” ai sensi degli artt. 7 e 13 della legge inglese sui brevetti del 1977 (*UK Patents Act 1977*) perché non è una persona fisica. La sentenza ha confermato le precedenti pronunce dell'*Intellectual Property Office* inglese (UKIPO) e della *High Court*, di fronte alla quale era stata impugnata la prima decisione.

La vicenda si inserisce nell'ambito della campagna internazionale di depositi di brevetto e ricorsi (“*Artificial Inventor Project*”) avviata dal Dr. Stephen Thaler a partire dal 2018, per sostenere la tesi che un sistema di intelligenza artificiale debba poter essere designato come inventore in una domanda di brevetto.

Il sistema di IA in questione, denominato “DABUS” (*Device for the Autonomous Bootstrapping of Unified Sentience*), creato dallo stesso Dr. Stephen Thaler e di proprietà della società statunitense *Imagination Engines Inc.*, avrebbe creato due dispositivi brevettabili che sono stati oggetto di domande di brevetto (oltre che a UKIPO) anche presso l'Ufficio Europeo dei Brevetti (EPO), lo *United States Patent and Trademark Office* (USPTO) e gli altri uffici brevetti nazionali ai sensi del Trattato di Cooperazione in materia di brevetti.

DABUS sarebbe costituito da due distinte reti neurali in grado di cooperare fra loro, elaborando concetti originali e sondandone la portata inventiva. Le due domande di brevetto riguardano, rispettivamente, un contenitore per alimenti e un particolare dispositivo di segnalazione. La prima concerne un contenitore per alimenti caratterizzato da un profilo frattale, che permette di adattarne la forma e lo rende particolarmente resistente; la seconda riguarda un dispositivo luminoso lampeggiante specificatamente ideato per far fronte a situazioni di emergenza.

Un unico filo conduttore attraversa queste domande: DABUS è nominato o dichiarato inventore, mentre il Dr. Thaler (il richiedente) è menzionato come proprietario del brevetto richiesto. Nelle domande depositate si precisa che il Dr. Thaler ha acquisito i diritti sul brevetto come proprietario, datore di lavoro e successore di DABUS.

Tra gli obiettivi del progetto c'è quello di incentivare l'innovazione utilizzando i sistemi di IA e raggiungere chiarezza, coerenza e certezza per i richiedenti di brevetti, soprattutto per quanto riguarda la questione di chi tra il proprietario, il programmatore o l'utente dell'IA

dovrebbe possedere il brevetto, riducendo la nomina impropria di persone come inventori che non si qualificano come tali.

Ad oggi, tra gli uffici dei brevetti che si sono pronunciati sulla richiesta del Dr. Thaler, solamente l'ufficio sud-africano (*South Africa's Companies and Intellectual Property Commission*) ha accolto la domanda, rilasciando in data 28 luglio 2021 il primo brevetto al mondo nel quale un sistema di IA sia designato come l'inventore, e il proprietario di tale sistema (ovvero il Dr. Thaler), sia designato come titolare del brevetto.

Le decisioni degli altri uffici brevetti che hanno respinto le domande, a causa del mancato rispetto dei requisiti formali delle rispettive legislazioni sui brevetti per non aver nominato una persona fisica come inventore, sono state successivamente impugnate dal Dr. Thaler.

Mentre la corte d'appello australiana ha riconosciuto (rinviando la decisione all'ufficio brevetti) che anche l'IA possa essere riconosciuta quale inventore, l'appello avverso le decisioni dell'UKIPO, oggetto della presente analisi e quello relativo alla decisione dell'USPTO sono stati respinti.

La pronuncia dell'ufficio brevetti sudafricano e quella della *Court of Appeal* australiana sono state citate dalla *Court of Appeal* inglese, ma non sono state prese in considerazione ai fini della decisione, dato che la Corte inglese si doveva soffermare solo sull'interpretazione della vigente normativa britannica.

La *Court of Appeal* inglese a maggioranza ha respinto l'appello (*Lord Justice Birss*, dissenziente) soffermandosi su tre aspetti fondamentali:

- 1) È necessario che un "inventore" sia una "persona"?
- 2) Il Dr. Thaler poteva richiedere dei brevetti per le invenzioni di DABUS?
- 3) Le domande presentate all'UKIPO dovevano essere considerate ritirate ai sensi dell'art. 13 del *Patents Act*?

In merito al primo quesito tutti i giudici hanno concordato che, ai sensi dell'art. 7 del *Patents Act 1977*, solo una persona possa essere designata come "inventore". Come già precisato nella giurisprudenza precedente (*Yeda Research and Development Company Ltd v. Rhone-Poulenc Rorer International Holdings* [2007] UKHL 43), l'art. 7 del *Patents Act 1977* chiarisce espressamente chi abbia diritto ad ottenere un brevetto.

L'articolo 7(2) stabilisce a chi possa essere concesso un brevetto: l'articolo 7(2)(a) si riferisce all'effettivo inventore, mentre l'articolo 7(2)(b) e l'articolo 7(2)(c) elencano le altre persone che possono avere titolo ad ottenere un brevetto in qualità di aventi causa ovvero in base a previsioni normative o contrattuali.

Dalla formulazione degli artt. 7(2) e 13 (2) nonché delle sezioni 2(4), 8 e 13(1) secondo i giudici della *Court of Appeal* risulta chiaro che solo una persona ne abbia diritto.

La seconda questione riguardava la possibilità per l'appellante di presentare domanda ai sensi dell'articolo 7(2)(b) del *Patents Act* per ottenere un brevetto.

Il Dr. Thaler sosteneva che, al momento della realizzazione delle invenzioni da parte di DABUS, avesse diritto ad esserne proprietario in virtù della dottrina dell'accessione descritta in *Blackstone's Commentaries on the Laws of England*, Ch. 26. Tuttavia, la casistica presa in considerazione da *Blackstone* riguarda nuovi beni materiali, che sono prodotti da beni materiali esistenti (ad es. i frutti degli alberi, la progenie degli animali).

Secondo tale dottrina, il proprietario del bene materiale preesistente è il proprietario del nuovo bene materiale, ma, come rilevato da *Lord Justice Arnold*, non c'è alcun riferimento all'applicazione della regola ai beni immateriali creati da beni materiali preesistenti; pertanto, nessuna norma stabilisce che il proprietario del sistema di IA sia proprietario delle invenzioni create da quest'ultima e non ha diritto a essere titolare del brevetto. A titolo esemplificativo,

*Lord Justice Arnold* richiama l'ipotesi in cui una persona A scatti una foto con la macchina fotografica digitale della persona B. In tal caso la persona A e non la persona B, proprietaria della macchina fotografica, sarà la titolare dei diritti sulla fotografia (sempre che tale opera possa essere considerata tutelata ai sensi del *Copyright, Designs and Patents Act* 1988).

Infine, in merito alla terza questione, relativa alla scelta dell'UKIPO di considerare ai sensi dell'art. 13(2), ritirate le domande perché il Dr. Thaler non aveva rispettato le prescrizioni del dettato normativo per la compilazione della domanda, *Lord Justice Birss* e *Lord Justice Arnold* hanno concordato che nel fare una dichiarazione ai sensi dell'articolo 13(2) del *Patents Act* 1977, il richiedente deve solo indicare chi ritiene essere l'inventore e una domanda di brevetto non sarà respinta per “*bona fide errors*”.

Su un punto la decisione, dei tre giudici della Corte d'Appello, non stata unanime: secondo *Lord Justice Birss* si doveva ritenere che il Dr. Thaler avesse presentato una dichiarazione a UKIPO, identificando al meglio delle sue convinzioni chi fosse l'inventore e il titolo derivativo di acquisto dei diritti, e pertanto, l'ufficio brevetti non avrebbe dovuto considerare ritirata la domanda. L'IPO non è tenuto ad effettuare una revisione sostanziale dell'accuratezza di qualsiasi dichiarazione. Chiunque ritenga di aver diritto ad ottenere un brevetto su quell'invenzione potrà in una fase successiva poter rivendicare il proprio diritto.

Gli altri due giudici del collegio, *Lord Justice Arnold* e *Lady Justice Laing*, invece, hanno ritenuto che mentre un controllo sostanziale dell'accuratezza di qualsiasi presentazione di informazioni ai sensi dell'articolo 13(2) non sia necessario, ciò è molto diverso dal consentire la valutazione di una domanda chiaramente non corretta. Dato che il Dr. Thaler non ha né identificato una persona come inventore nelle informazioni fornite a UKIPO né fornito un titolo derivativo valido, anche una valutazione superficiale avrebbe consentito di valutarla irricevibile ai sensi della legge.

La pronuncia della *Court of Appeal* potrebbe essere impugnata di fronte *Supreme Court*, tuttavia, potrebbe non sortire il risultato atteso dall'appellante, considerando che, come sottolineato da *Lord Justice Arnold*, molte argomentazioni contenute nell'appello del Dr. Thaler sono state proposte per una normativa futura e non prendono in considerazione le attuali norme vigenti (“*frequently put on the basis of what the law ought to be rather than it was*”).

Da considerare che il giorno dopo la sentenza della *Court of Appeal*, il governo britannico ha pubblicato la sua “*National AI Strategy*”, annunciata come “un nuovo piano decennale, per rendere il Regno Unito una superpotenza globale di IA”. Nell'ambito di questa iniziativa, l'UKIPO lancerà nei prossimi tre mesi una consultazione sull'utilizzo degli IPRs per proteggere l'IA, da cui potrebbe derivare una soluzione legislativa.

Negli ultimi anni è evidente l'impatto dell'IA sulla proprietà intellettuale, o per meglio dire, sui sistemi di protezione basati sulla concessione di diritti esclusivi a fronte di un atto creativo o inventivo.

Il problema si pone per le cd. “*AI Generated Works*”, opere dell'ingegno per le quali, come per le invenzioni presentate dal Dr. Thaler, l'intervento umano è insignificante o del tutto assente: è possibile (ed opportuno) qualificare tali contenuti creativi e/o inventivi come proteggibili e a chi devono essere riconosciuti i relativi diritti. *Nulla quaestio*, invece, per le cd. “*AI Assisted Works*”, opere create da persone fisiche ove l'IA è usata come strumento: in tal caso sarà la persona fisica ad essere considerata quale autore/inventore e titolare dei diritti.

Attualmente la maggior parte degli ordinamenti nazionali stabiliscono che le opere dell'ingegno e le invenzioni siano tutelate solo se create da persona fisica e la titolarità dei diritti non possa essere riconosciuta in capo all'IA: pertanto, se le opere creative e/o inventive sono create da IA non saranno tutelate e cadranno in pubblico dominio.

Date le opinioni divergenti dei giudici della *Court of Appeal* inglese, nonché dei togati delle altre corti che si sono pronunciate, risulta evidente che si tratta di un'importante area del

diritto che non è stata ancora oggetto di interventi legislativi ma che meriterebbe di essere disciplinata nel prossimo futuro dai *policy makers*.

FRANCESCO GROSSI

<https://www.judiciary.uk/wp-content/uploads/2021/10/Thaler-v-Comptroller-judgment.pdf>

2021/4(7)FDA

**La sentenza del Tar Lazio n. 7589 del 24 giugno 2021 su algoritmi e attività amministrativa (a proposito di procedure di mobilità nella Pubblica Amministrazione)**

La vicenda decisa dalla sentenza del TAR Lazio – sede di Roma, Sez. III-bis, 24 giugno 2021, n. 7589 trae origine da una procedura di mobilità nazionale all'esito della quale il Ministero dell'università e della ricerca (MIUR) ha negato ai ricorrenti – tutti docenti di sostegno in servizio presso istituti scolastici – il trasferimento in altra sede di lavoro per mancanza di un requisito oggettivo (la permanenza quinquennale nella sede d'origine) non richiesto né applicato ad altri candidati.

Risolta la questione preliminare di giurisdizione in favore del giudice amministrativo, la causa è stata trattenuta in decisione dal collegio che ha accolto il ricorso collettivo per evidente disparità di trattamento.

Il TAR Lazio ha evidenziato che il nucleo centrale della questione risiede nel fatto che l'amministrazione centrale ha deciso di gestire tutto il procedimento di mobilità attraverso un algoritmo che ha inficiato la regolarità del concorso e leso la sfera giuridica dei candidati.

Nell'accogliere l'impugnativa, il giudice romano ha notato come sia *“mancata nella fattispecie una vera e propria attività amministrativa”* dal momento che il Ministero ha devoluto a un *“impersonale”* (e quindi privo di componente umana) sistema informatico lo svolgimento della procedura di assegnazione dei docenti alle sedi lavorative disponibili in base all'organico scolastico.

L'ingente numero di concorrenti alla procedura di mobilità non poteva rappresentare un incentivo in tal senso; né consentiva di usare in via esclusiva un meccanismo matematico privo delle capacità valutative richieste per gestire la *“tradizionale e garantistica istruttoria procedimentale”* che deve informare l'attività amministrativa.

Secondo il TAR laziale un algoritmo – quand'anche impostato per tenere conto delle singole posizioni personali, dei titoli e dei punteggi – non può fornire adeguate garanzie di partecipazione e trasparenza al privato che si confronta col pubblico potere; e finisce per soppiantare l'attività umana con quella asettica di un calcolatore che non può mai svolgere una *“attività”* in senso stretto, non essendo il *“prodotto delle azioni dell'uomo”*.

Così facendo l'amministrazione ha violato l'obbligo di motivazione delle decisioni amministrative e il correlato diritto alla tutela giurisdizionale perché l'assenza di un'attività amministrativa in senso specifico non ha permesso agli interessati e poi al giudice di ricostruire il percorso logico seguito dall'amministrazione per giungere alle sue determinazioni provvedimenti.

In conclusione, il TAR ha stigmatizzato l'utilizzo improprio di *“procedure informatizzate”* che eludono le regole generali dell'attività amministrativa. Il ricorso a un algoritmo rappresenta un *“modulo organizzativo”* (più di preciso uno *“strumento procedimentale ed istruttorio”*)

che, in ossequio al principio di legalità amministrativa, dev'essere regolato dalla legge e deve rispondere rigorosamente alle finalità da questa indicate.

FILIPPO D'ANGELO

<https://www.giustizia-amministrativa.it/dcsnpr>

2021/4(8)VR

**L'ordinanza del 16 settembre 2021 del Garante Privacy a proposito del sistema software di supervisione degli studenti "Respondus" impiegato dall'Università Bocconi di Milano per le prove scritte di esame**

Il 16 settembre 2021 il Garante per la protezione dei dati personali ( "Garante Privacy" o l' "Autorità") ha dichiarato l'illiceità del trattamento effettuato dall'Università Commerciale "Luigi Bocconi" di Milano (di seguito, la "Università") a mezzo di un sistema software di supervisione (*proctoring*) impiegato dall'Università nell'ambito dell'espletamento delle prove scritte d'esame al fine di identificare gli studenti e di verificarne il corretto comportamento, con conseguente adozione *inter alia* di provvedimenti ai sensi degli artt. 2-*decies* del d.lgs. n. 196/2003 ( "Codice Privacy") e 58, par. 2 del Regolamento UE n. 2016/679 ("GDPR").

In risposta all'impossibilità di sostenere gli esami in presenza dovuta all'emergenza epidemiologica da SARS-CoV 2, l'Università adottava, come modalità alternativa, lo svolgimento di prove scritte a distanza, la cui genuinità sarebbe stata garantita dall'impiego del software "Respondus" quale sistema di *proctoring*. Nello specifico, tale *software*, tra le altre funzionalità, inibiva anzitutto l'utilizzabilità del *browser* da parte dello studente, procedendo quindi, tramite la sua articolazione "Respondus Monitor", a catturare le immagini video e lo schermo degli esaminandi e a individuarne eventuali condotte sospette, mediante registrazione video e acquisizione di istantanee a intervalli regolari. Quest'ultime, debitamente contrassegnate, venivano poi messe a disposizione dei docenti, cui erano riservate le valutazioni in merito.

Snodo centrale nel *rationale* del provvedimento è l'affermazione dell'assenza di un'ideale base giuridica per i trattamenti posti in essere mediante il menzionato sistema di supervisione. *In primis*, nonostante l'Università avesse negato, con apposita rettifica in sede di memorie difensive, l'avvenuta estrazione di campioni biometrici, l'operatività del *software* "Respondus Monitor" (raccolta, elaborazione e analisi dei video acquisiti tramite apposito algoritmo, con eventuale *flag* dei comportamenti anomali) veniva qualificata dal Garante come trattamento di dati biometrici, secondo la definizione dell'art. 4, par. 1, n. 14 del GDPR ("i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici") relativi all'immagine facciale degli studenti. L'Autorità, inoltre, richiamava il proprio provv. 26 luglio 2017, n. 345, nel quale si ammoniva che "nel caso del riconoscimento facciale, il presupposto perché il trattamento delle immagini possa essere qualificato come trattamento biometrico è che i confronti finalizzati al riconoscimento dell'individuo (...) siano automatizzati mediante l'ausilio di appositi strumenti software o hardware". Com'è noto, la delicatezza di tale categoria di dati personali ne fonda l'inclusione tra i cc.dd. dati particolari, destinatari dell'elevata protezione offerta dall'art. 9 del GDPR che, a fronte di un generale divieto, ne autorizza il trattamento alle sole condizioni *ivi* previste "ed in conformità alle misure di garanzia disposte dal

*Garante*". Ebbene, la base giuridica dei trattamenti veniva individuata dall'Università nel consenso del singolo studente, al quale era comunque espressamente concessa, in caso di rifiuto, la possibilità di sostenere la prova con modalità alternative da concordare col docente. Alla delimitazione della base giuridica del consenso, il Garante Privacy ha opposto due obiezioni, in primo luogo affermando che tale base non può invocarsi nemmeno in astratto laddove il trattamento sia (come nel caso di specie) finalizzato al rilascio di titoli di studio aventi corso legale, posto che tale attività integra il perseguimento di una finalità di interesse pubblico sprovvista di una adeguata normazione in punto di previsione di garanzie degli interessati, ai sensi dall'art. 9, par. 2 lett. g) del GDPR e dell'art. 2-*sexies* del Codice Privacy; e, in secondo luogo, obiettando che in ogni caso, nella fattispecie concreta, il consenso degli studenti non era libero. Quanto a quest'ultimo aspetto, il Garante Privacy ha ritenuto che nella fattispecie concreta, era difettata una "manifestazione di volontà libera" ex art. 4, par. 1, n. 11) del GDPR, in ragione dello squilibrio della posizione degli studenti rispetto al titolare del trattamento, richiamando in proposito il Considerando n. 43 del GDPR, e motivando ulteriormente l'esistenza dello squilibrio con la possibilità che il sistema adottato dall'Università generasse negli studenti il "*timore di subire ripercussioni negative, anche indirette, da parte dei docenti come conseguenza del rifiuto*". Quanto al primo aspetto, il Garante Privacy sembra aver instaurato un rapporto di prevalenza, in favore della seconda, tra le due basi di esclusione del divieto di cui alle lettere a) (consenso) e g) (motivi di interesse pubblico normati in punto di garanzia per gli interessati) di cui al par. 2 dell'art. 9 del GDPR, nel senso di ritenere unicamente rilevante accertare la sussistenza delle condizioni per l'esclusione del divieto per motivi di interesse pubblico, ricorrendo simili motivi, ed irrilevante la base del consenso. In particolare, il Garante Privacy ha osservato che l'elemento cardine che consente l'esercizio della libertà di insegnamento (art. 33 Cost. e art. 1 l. 30 dicembre 2010, n. 240) tanto a soggetti pubblici quanto a privati risiede nel perseguimento di finalità di interesse pubblico e che, per tale ragione, la base giuridica dei trattamenti in questione andava correttamente ricercata nell'art. 9, par. 2, lett. g) del GDPR, non potendo, per contro, rinvenirsi tale base nel consenso e/o nel contratto. Ai sensi della citata disposizione di cui alla lett. g) del par. 2 dell'art. 9 GDPR, il divieto di cui al par. 1 del medesimo articolo non opera se "*il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*". Tale prescrizione è poi ulteriormente declinata e precisata all'art. 2-*sexies* del Codice Privacy (come modificato ad opera del d.lgs. 10 agosto 2018, n. 101), che subordina l'ammissibilità dei trattamenti di dati particolari necessari per motivi di interesse pubblico alla previsione nell'ordinamento domestico di apposite "*disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*".

Ciò premesso, constatato il difetto, nella legislazione italiana, di una norma in grado di soddisfare le illustrate garanzie, il Garante Privacy concludeva per l'assenza di un'adeguata base giuridica a fondamento dei trattamenti di dati biometrici effettuati dall'Università mediante il software "*Respondus*", in violazione degli artt. 5, 6 e 9 del GDPR e dell'art. 2-*sexies*, comma 1, del Codice Privacy. Inoltre, le predette argomentazioni venivano riproposte nel provvedimento per sostenere l'illiceità dei trattamenti anche alla luce della qualificabilità delle operazioni poste in essere dal sistema di *proctoring* come produttive di una "profilazione" degli studenti. Infatti, nonostante la valutazione di merito circa le condotte degli studenti fosse rimessa ai docenti, l'oggetto di tale giudizio era formato, secondo i rilievi del Garante Privacy, dalle sole ipotesi previamente analizzate e contrassegnate dall'algoritmo, integrando così, ad avviso della medesima Autorità, un "*trattamento automatizzato di dati personali (...) per valutare*

*determinati aspetti personali relativi a una persona fisica*” sussumibile nell’ampia definizione di “profilazione” di cui all’art. 4, par. 1, n. 4 del GDPR. Secondo il Garante Privacy, i pericoli che ne derivano si compendiano essenzialmente nel rischio di generare informazioni diverse e ulteriori rispetto a quelle fornite dall’interessato.

Tale ultimo aspetto, ad avviso del Garante Privacy si è concretamente verificato nel caso di specie, posto che è risultato che “Respondus Monitor” teneva traccia dell’attività dell’esaminando durante la seduta (disconnessioni dalla rete Internet; tentativi di utilizzare il mouse o il trackpad per passare da un’applicazione all’altra o per uscire dal sistema; applicazioni in uso; posizione del viso dello studente). Da ciò l’ulteriore questione del rispetto dei principi di minimizzazione e di limitazione della conservazione di cui all’art. 5, lett. c) ed e) del GDPR. Ai sensi dell’art. 25 del GDPR, essi devono essere attuati dal titolare del trattamento “*fin dalla progettazione*” e “*per impostazione definita*”, anche in caso di impiego di prodotti o servizi realizzati da terzi. Ebbene, ad avviso dell’Autorità, con riferimento al principio di minimizzazione, i dati personali prodotti dalla profilazione sono risultati sovrabbondanti e non necessari per garantire il regolare svolgimento della prova e la sua validità. Per quanto concerne la durata di conservazione delle informazioni, anche in ossequio al principio dell’*accountability*, il Garante Privacy ha osservato che è prescritta un’esplicitazione *ex ante* in maniera certa e documentabile, essendo insufficiente tanto il mero riferimento alla facoltà per l’Università di chiedere in qualsiasi momento la cancellazione dei dati, prevista nell’accordo sul trattamento stipulato col fornitore, quanto il suo esercizio al termine delle sessioni d’esame e del procedimento di valutazione delle prove. La genericità di tali indicazioni, secondo l’Autorità, non consentiva peraltro una corretta informazione preventiva dell’interessato né una compiuta “*valutazione delle necessità e proporzionalità dei trattamenti in relazione alle finalità*” (art. 35, par. 7, lett. b) del Regolamento), anche con riguardo alla “*limitazione della conservazione (articolo 5, paragrafo 1, lettera e)*”. Per tali ragioni, il Garante Privacy rilevava l’illiceità del trattamento per violazione degli artt. 5, par. 1, lett. c) ed e) e 25 del GDPR.

Gli illustrati profili di illiceità, come emerge dal punto precedente, si riverberano sull’obbligo di informazione preventiva di cui è gravato il titolare del trattamento ai sensi degli artt. 5, par. 1, lett. a), 12 e 13 del GDPR, attuativo del principio di liceità, correttezza e trasparenza. In proposito, l’Autorità ha rilevato che l’informativa fornita agli studenti dall’Università risultava gravemente incompleta, anzitutto per aver omesso di menzionare diverse forme di trattamento operate dal sistema “Respondus” quali: il tracciamento delle condotte durante la seduta d’esame, le successive elaborazioni mediante profilazione (cfr. Considerando n. 60 del GDPR), la registrazione audio-video della prova, l’acquisizione di un’istantanea dell’interessato all’inizio della prova. Inoltre, come già evidenziato, l’Autorità ha ritenuto difettare una precisa indicazione delle tempistiche di conservazione dei dati acquisiti. Infine, il Garante Privacy rilevava che non veniva fatto riferimento alcuno al trasferimento dei dati personali in ordinamenti extra-UE – nel caso di specie, nell’ordinamento USA, ove ha sede la società Respondus Inc., fornitore del servizio e responsabile del trattamento – e, *a fortiori*, alla base giuridica dello stesso. Peraltro, l’Autorità affermava che le carenze tratteggiate non potevano ritenersi “compensate” dal rinvio, mediante *link* ipertestuale inserito nell’informativa, a pagine *web* dell’Università deputate genericamente a illustrare i trattamenti effettuati con riguardo alla “*esperienza scolastica, accademica o professionale, al titolo della tesi, al titolo del progetto finale, alla durata degli studi e ai risultati degli esami [nonché alla] documentazione sulla valutazione del vostro lavoro*”, né tantomeno dalla rappresentazione in forma orale del funzionamento del *software* “Respondus” ai soli rappresentanti degli studenti. Alla deficienza del compendio informativo fornito agli interessati, poi, si accompagnava una presentazione “*frammentaria e disorganica*”. Ciò conduceva

il Garante a rilevare la non conformità dei trattamenti al principio di liceità, trasparenza e correttezza, in violazione degli artt. 5, par. 1, lett. a), e 13 del GDPR.

Un ulteriore profilo di illiceità concerneva (oltre che la relativa informativa, di cui si è detto *supra*) la stessa esportazione dei dati acquisiti nell'ordinamento USA (ove, come detto, è stabilita la società *Respondus Inc.*, responsabile del trattamento). Com'è noto, ai sensi dell'art. 44 del GDPR, i trasferimenti internazionali sono ammessi solo nel rispetto delle condizioni previste agli artt. 45-49 del GDPR, così articolate: le decisioni di adeguatezza assunte dalla Commissione europea (art. 45) all'esito di un giudizio olistico di equivalenza sostanziale dell'ordinamento straniero sul livello di protezione dei dati personali; la prestazione di adeguate garanzie da parte del titolare del trattamento (artt. 46 e 47), fra cui spiccano le clausole tipo adottate dalla Commissione europea, oltre alle norme vincolanti d'impresa; infine, le deroghe *ex art.* 49, accessibili solo “*in caso di trasferimenti occasionali e non ripetitivi*” (cfr. le “Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679”, adottate il 25 maggio 2018 dal Comitato europeo per la protezione dei dati). In data 16 luglio 2020, la c.d. sentenza *Schrems II* della Corte di Giustizia dell'Unione Europea (causa C-311/18) dichiarava invalida la decisione di adeguatezza n. 2016/1250, che avallava il c.d. *Privacy Shield* statunitense e suggellava la sostanziale equivalenza degli ordinamenti USA e UE in punto di protezione dei dati personali [sul punto v. la notizia [2020/3\(1\)CR](#)]. Caduto tale canale preferenziale, l'originario accordo tra l'Università e la *Respondus Inc.*, non potendo più fondare il trasferimento sull'adesione dell'impresa al *Privacy Shield*, veniva emendato mediante ricorso, con un atto aggiuntivo *ad hoc*, alle clausole contrattuali tipo avallate dalla Commissione europea con la decisione n. 2010/87 del 5 febbraio 2010. Tuttavia, l'Autorità rilevava che il rinnovato accordo ometteva di indicare le misure tecniche e organizzative di sicurezza predisposte dall'importatore, la cui descrizione era accessibile esclusivamente a seguito di apposita richiesta inoltrata attraverso uno specifico modulo *online*. Di più. Secondo il Garante Privacy, l'Università, di fatto, non era neppure in grado di aver contezza delle misure effettivamente adottate dall'importatore nei singoli trattamenti. Ciò – rilevava l'Autorità - si poneva anzitutto in contrasto con gli artt. 4, par. 1, lett. c) e 5, lett. c) delle clausole standard ma soprattutto, in tal modo, gli interessati erano privati del tutto della facoltà di far valere nei confronti dell'esportatore gli impegni contrattualmente assunti in materia di sicurezza, in violazione dell'art. 3, par. 1 delle clausole tipo allegato alla citata decisione n. 2010/87. Tali rilievi, da ultimo, portavano il Garante Privacy a ritenere che il descritto *deficit* contenutistico che inficiava *in parte qua* l'accordo tra l'Università e la *Respondus Inc.* rivelasse l'assenza di una previa verifica dell'esportatore circa l'effettiva capacità delle misure poste dall'importatore a garanzia del rispetto degli obblighi di protezione assunti. Le suesposte argomentazioni venivano poste alla base della declaratoria di illiceità dei trasferimenti in oggetto per violazione degli artt. 44 e 46 del GDPR.

L'ultimo aspetto affrontato dal Garante Privacy riguarda la valutazione di impatto sulla protezione dei dati personali (DPIA), che il titolare del trattamento è tenuto a effettuare ove “*un tipo di trattamento, allorché preved[a] in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, [possa] presentare un rischio elevato per i diritti e le libertà delle persone fisiche*” (art. 35 del GDPR)”. Secondo l'Autorità, la valutazione dell'Università si dimostrava inadeguata, succinta e non puntuale, tanto nella verifica della necessità e della proporzionalità dei trattamenti in relazione alle finalità (massimamente, sotto il profilo dell'eccessività della “profilazione”) quanto nell'analisi dei rischi e nella conseguente adozione di misure appropriate.

In conclusione, l'insieme dei rilievi trattenuti conduceva il Garante Privacy, *inter alia*, a dichiarare l'illiceità dei trattamenti posti in essere dall'Università per violazione degli artt. 5, par. 1, lett. a), c) ed e), 6, 9, 13, 25, 35, 44 e 46 del GDPR, nonché 2-*sexies* del Codice Privacy;

dichiarare la conseguente inutilizzabilità dei dati personali trattati, ai sensi dell'art. 2-*decies* del Codice Privacy; disporre, nell'esercizio dei poteri correttivi di cui all'art. 58, par. 2, lett. *f*) del GDPR, la limitazione del trattamento, vietando all'Università ogni ulteriore operazione di trattamento con riguardo ai dati biometrici degli studenti e ai dati sulla cui base viene effettuata la profilazione degli interessati mediante il sistema “*Respondus*”, nonché vietando il trasferimento dei dati personali degli interessati negli Stati Uniti d'America in assenza di adeguate garanzie per gli stessi; ingiungere all'Università il pagamento della somma di euro 200.000,00 a titolo di sanzione amministrativa pecuniaria *ex* artt. 58, par. 2, lett. *z*) e 83, par. 5 del GDPR (e fatta salva la facoltà di pagamento dell'importo ridotto *ex* art. 166 co. 8 del Codice Privacy).

VALENTINO RAVAGNANI

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9703988>

2021/4(9)ES

### **L'apertura della prima finestra temporale sulla sandbox regolamentare per i progetti fintech di cui al Decreto del MEF n. 100 del 30 aprile 2021**

Il 30 settembre 2021 la Banca d'Italia, la Consob e l'Ivass (da ora anche le “**Autorità di vigilanza**” o le “**Autorità**”) hanno diffuso un comunicato stampa congiunto in cui annunciavano l'avvio della prima finestra temporale, dal 15 novembre 2021 al 15 gennaio 2022, per presentare le richieste di ammissione alla sperimentazione fintech nell'ambito della sandbox regolamentare.

Il comunicato dà seguito al Decreto del Ministero dell'economia e delle finanze n. 100 del 30 aprile 2021 (da ora anche il “**Regolamento *sandbox***”) entrato in vigore il 17 luglio 2021 in attuazione della delega conferita con l'art. 36, commi 2 *bis* e ss. D. L. n. 34/2019 (c.d. “Decreto crescita”) e disciplinante proprio la menzionata sperimentazione.

La *sandbox* regolamentare è un ambiente controllato dove gli operatori del settore, come definiti *infra*, possono sviluppare progetti innovativi in ambito bancario, finanziario e assicurativo sotto la vigilanza e con il supporto delle competenti Autorità. La *sandbox* intende incentivare l'adozione di soluzioni tecnologiche e il loro ordinato impiego nei suddetti settori. La costante sorveglianza delle Autorità, da un lato, tutela la stabilità finanziaria, gli interessi dei consumatori e dei concorrenti e il buon funzionamento del mercato. Dall'altro, consente alle medesime Autorità di monitorare l'evoluzione del mercato e gestire sin da subito eventuali nuovi rischi associati all'impiego delle soluzioni in fase di sperimentazione.

Il Regolamento *sandbox* precisa che i partecipanti a quest'ultima possono essere operatori fintech, ossia soggetti, pure non vigilati, che svolgano o intendano svolgere attività fintech anche in misura non prevalente (art. 1). Possono partecipare anche intermediari vigilati dalle competenti Autorità e con sede legale o succursale in Italia ovvero con sede legale negli Stati membri dell'UE ed operanti in Italia in regime di libera prestazione di servizi. Sono esclusi dalla partecipazione alla *sandbox* coloro i quali siano assoggettati ad una procedura concorsuale o non abbiano depositato il bilancio negli ultimi 5 anni.

La soluzione da sperimentare deve riguardare i settori bancario, finanziario o assicurativo ed essere: i) “*soggetta all'autorizzazione o all'iscrizione in un albo, elenco o registro da parte di almeno una delle autorità di vigilanza*”, oppure esentata dalla suddetta iscrizione; ii) prestata “*in favore di un soggetto vigilato o regolamentato da almeno un'autorità di vigilanza ... avente in Italia la propria sede legale*”

o una succursale”, ovvero in favore di un ente con sede legale negli Stati membri dell’UE ed operante in Italia in regime di libera prestazione di servizi; iii) “svolta da un soggetto vigilato o regolamentato da almeno un’ autorità di vigilanza ... avente in Italia la propria sede legale o una succursale”, ovvero da un ente con sede legale negli Stati membri dell’UE ed operante in Italia in regime di libera prestazione di servizi” (art. 5).

Per essere ammesse alla sperimentazione, è altresì necessario che l’attività: i) sia “significativamente innovativa”, ossia avvalendosi delle nuove tecnologie fornisca prodotti o servizi prima non esistenti, oppure oggettivamente diversi da quelli già noti, nei settori bancario, finanziario o assicurativo. È altresì innovativa la soluzione che utilizzi tecnologie già in uso in nuovi modelli di business; ii) presupponga una deroga ai provvedimenti adottati dalle Autorità di vigilanza; iii) crei valore aggiunto tanto per gli utenti quanto per il mercato; iv) sia in uno stato di sviluppo talmente avanzato da consentire la sperimentazione; v) sia economicamente sostenibile (art. 6).

È possibile stabilire un numero massimo di progetti ammissibili alla sperimentazione, che non può durare più di diciotto mesi, salvo proroghe concesse dall’Autorità di vigilanza. Coloro i quali siano interessati a partecipare, e necessitino di chiarimenti, possono avviare dei colloqui informali preliminari alla presentazione della domanda beneficiando del supporto delle Autorità (art. 8). Dopo aver presentato la richiesta di ammissione, la Banca d’Italia, l’Ivass e la Consob, singolarmente o congiuntamente a seconda dell’ambito di applicazione del progetto presentato, condurranno un’istruttoria (art. 12), comunicandone gli esiti al Comitato fintech. Quest’ultimo, ai sensi del citato Regolamento *sandbox*, monitora l’evoluzione del settore fintech sia a livello nazionale che sovranazionale, formula proposte normative, agevola l’interlocuzione tra gli operatori di settore e le Autorità che decidono sull’ammissione alla sperimentazione. L’ammissione è comunicata al partecipante, comporta la sua iscrizione in apposito registro tenuto dal Comitato ed è revocabile nei casi di cui all’art. 14, comma 1, lett. d) Regolamento *sandbox*.

Durante la sperimentazione ciascuna Autorità vigila sulle attività svolte e può adottare i provvedimenti di cui agli artt. 13 e 14 Regolamento *sandbox* per il proprio settore di competenza, inclusa soprattutto la deroga per diciotto mesi, salva diversa disposizione, alla regolamentazione emanata dalla stessa Autorità di vigilanza.

Per disciplinare gli incumbenti nascenti dal citato Regolamento *sandbox* la Banca d’Italia, la Consob e l’IVASS hanno emanato ciascuna un proprio regolamento (da ora anche i “**Regolamenti**”) disciplinante l’emanazione, per quanto di competenza, dei provvedimenti di ammissione alla *sandbox*. Si tratta rispettivamente: del Regolamento di Banca d’Italia del 3 novembre 2021, pubblicato sulla G.U. del 10 novembre 2021; della delibera Consob n. 22054 del 27 ottobre 2021, pubblicata sulla G.U. del 5 novembre 2021 e del regolamento IVASS n. 49 del 3 novembre 2021 pubblicato sulla G.U. del 13 novembre 2021. I Regolamenti sono pressoché equivalenti tra di loro, differenziandosi solo per le Autorità di cui disciplinano l’azione, consentendo una trattazione congiunta e non introducono significative novità rispetto al Regolamento *sandbox*.

Per quanto da essi non espressamente disciplinato si applicano i regolamenti generali sui procedimenti amministrativi delle rispettive Autorità (art. 1). Tutti i Regolamenti individuano le unità organizzative responsabili del procedimento di ammissione alla sperimentazione nel loro Allegato I (art. 3) e i requisiti che deve avere la relativa domanda (art. 5). Come già stabilito nel Regolamento *sandbox*, le Autorità potranno chiedere chiarimenti e integrazioni agli interessati sulle domande da loro presentate che, in caso di inottemperanza alla richiesta nel termine stabilito (art. 6), sono rigettate. Anche l’istruttoria e la conclusione del procedimento di ammissione (artt. 7 - 10) sono disciplinati similmente al Regolamento *sandbox*. A partire da tali fasi, inoltre, ciascuna Autorità di vigilanza può chiedere la

formulazione di un parere al Comitato fintech o ad un'altra di esse per i settori di rispettiva competenza. Infine, tanto la proroga e la conclusione del periodo di sperimentazione (artt. 13 e 16), quanto la revoca dell'ammissione a quest'ultima (artt. 14 e 15), su istanza di parte o d'ufficio, sono disciplinati analogamente al Regolamento *sandbox*, seppur con maggior dettaglio.

EMANUELE STABILE

<https://www.bancaditalia.it/focus/sandbox/index.html>

2021/4(10)AF

### **Il rapporto del 13 ottobre 2021 dei Ministeri dell'Economia e delle Banche Centrali dei Paesi G7 "Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)"**

Il 13 ottobre 2021 i Ministeri dell'Economia e le Banche Centrali dei Paesi G7 hanno pubblicato il rapporto "*Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)*" (**"il Rapporto"**). Il Rapporto si propone di delineare dei principi generali da considerare nella ideazione e configurazione di una *Retail Central Bank Digital Currency* (**"CBDC retail"**).

Una *CBDC retail* costituirebbe una forma di moneta di banca centrale digitale direttamente accessibile al pubblico e destinata a un uso diffuso. Funterebbe, quindi, da complemento al contante. Il Rapporto non esclude comunque iniziative volte allo sviluppo di *CBDC wholesale*, vale a dire una *CBDC* il cui uso sarebbe limitato ai pagamenti all'ingrosso e il cui accesso sarebbe ristretto alle sole istituzioni finanziarie regolamentate.

Il Rapporto è il risultato di una più ampia fase di indagine avviata nel giugno 2021 dai Ministeri dell'Economia e Banche Centrali G7 sulle implicazioni dello sviluppo di una *CBDC retail*. Si tratta di principi che dovrebbero fungere da guida. Il G7 riconosce, infatti, che la decisione sull'emissione e configurazione di una *CBDC* è competenza delle autorità nazionali. Tuttavia, il Rapporto evidenzia anche come dei principi comuni potrebbero affermare alcuni valori condivisi rilevanti, quali trasparenza, aderenza al quadro normativo e buon governo economico.

Il Rapporto delinea, in particolare, tredici principi a cui la configurazione e lo sviluppo di una *CBDC retail* dovrebbero ispirarsi, tenendo conto sia delle *foundational issues* che una *CBDC* dovrebbe fronteggiare (es. mantenimento di un adeguato livello di competizione nell'ambito dei pagamenti digitali), sia delle *opportunities* che ne potrebbero scaturire. Tra le *opportunities*, il Rapporto segnala come le *CBDCs* potrebbero promuovere l'innovazione digitale, stimolare una maggiore inclusione finanziaria e favorire la conduzione di transazioni *cross-border*. Focus del rapporto sono anche le *dependencies* che potrebbero sussistere tra i diversi principi. Il G7 riconosce come un approccio *one size fits all* non sia perseguibile, sicché la configurazione e sviluppo di una *CBDC* dovrà aversi in ciascun caso rispetto agli specifici obiettivi che si intendono conseguire, tenendo sempre però conto dei valori e dei principi generali.

Una *CBDC* dovrebbe, *in primis*, preservare la stabilità monetaria e finanziaria, consentendo alle banche centrali di adempiere al proprio mandato. In particolare, le *CBDCs retail* potrebbero rafforzare il ruolo della moneta di banca centrale e assicurare la fiducia del pubblico. Al contempo, però, le *CBDCs* potrebbero anche comportare alcuni rischi per il

sistema finanziario e, in particolare, bancario, quali, fra tutti, il rischio di sostituzione dei depositi.

Una CBDC dovrebbe, poi, proteggere la *privacy* degli utilizzatori, garantendo trasparenza circa il trattamento e l'uso dei dati. Al contempo, una CBDC e il relativo ecosistema dovrebbero anche assicurare la prevenzione e il contrasto del riciclaggio e del finanziamento del terrorismo. Nel Rapporto si suggeriscono diversi modelli volti a individuare una soluzione di equilibrio, quali, ad esempio, CBDC *account* pseudo anonimi basati su tecnologie DLT.

Una CBDC e il relativo ecosistema dovrebbero essere strutturati in modo tale da minimizzare i rischi operativi e informatici, nonché da garantire efficienza energetica. Si riconosce, però, come *standard* stringenti di resilienza operativa e sicurezza potrebbero impattare sulla *performance* e la funzionalità dell'ecosistema. Un giusto equilibrio dovrà essere, quindi, individuato.

Particolare attenzione, poi, è posta ai rischi che una CBDC potrebbe avere sulla competizione nell'ambito dei pagamenti digitali. Una CBDC dovrebbe coesistere con i mezzi di pagamento esistenti, promuovendo competizione e diversità. Al riguardo, si evidenzia come sia necessario assicurare interoperabilità tra le diverse soluzioni di pagamento. Non solo, nello *statement* congiunto del G7 viene rimarcato anche come le CBDCs dovrebbero coesistere con le nuove forme private di moneta digitale- quali in particolare, gli *stablecoin*- fintantoché tali forme siano coerenti con gli obiettivi di *policy* delineati. Ne vengono, difatti, evidenziate le differenze, essendo gli *stablecoin* passività di soggetti privati che ambiscono a mantenere un valore stabile, senza però che ve ne sia certezza. Considerati i rischi significativi, il G7 rimarca come sia necessario assicurare *standard* comuni di regolamentazione da delineare secondo il principio *same activity, same risk, same regulation*.

Altrettanta rilevanza è attribuita all'uso delle CBDCs in ambito *cross-border* e, in particolare, ai rischi che ne potrebbero derivare per la stabilità monetaria e finanziaria internazionale. Secondo il Rapporto, da tenere in considerazione è il rischio per cui l'uso di una CBDC sia così significativo negli altri Paesi da determinare una sostituzione della valuta. Rischi del genere dovrebbero essere, però, soppesati dai benefici che una dimensione internazionale di una CBDC potrebbe apportare nella conduzione delle transazioni *cross-border*. Al riguardo, si sottolinea come forme di integrazione e cooperazione siano necessarie, anche con riferimento a iniziative di sviluppo internazionale.

Infine, una CBDC dovrebbe essere delineata in modo tale da incrementare l'inclusione finanziaria e non impedire, ma, anzi, ampliare l'accesso ai servizi di pagamento, anche con riferimento a un possibile impiego delle CBDC nei pagamenti da e verso il settore pubblico.

Alice Filippetta

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1025235/G7\\_Public\\_Policy\\_Principles\\_for\\_Retail\\_CBDC\\_FINAL.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025235/G7_Public_Policy_Principles_for_Retail_CBDC_FINAL.pdf)

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1025234/FINAL\\_G7\\_Statement\\_on\\_Digital\\_Payments\\_13.10.21.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025234/FINAL_G7_Statement_on_Digital_Payments_13.10.21.pdf)

2021/4(11)SS

## Le classi di rischio dei ‘Software As Medical Device’ (SAMDs) alla data di piena applicazione del Regolamento 2017/745 UE sui dispositivi medici

Il **Regolamento (UE) 2017/745** sui dispositivi medici (*Medical Device Regulation*, di seguito “**MDR**”) – entrato in vigore con data di piena applicazione il 26 maggio 2021 – è incentrato sul *risk approach* e sull’implementazione del sistema di gestione del rischio, del sistema di monitoraggio post-vendita e del sistema di vigilanza.

L’attenzione è infatti focalizzata sulla sicurezza e l’efficacia dei dispositivi. Viene stabilita in capo ai produttori una responsabilità per il controllo sulla produzione e sulla commercializzazione dei dispositivi. Rispetto all’impianto normativo previgente, alcune tra le principali novità possono essere così sintetizzate.

Il MDR amplia l’ambito di applicazione della nozione prevista dalla Direttiva 93/42/CEE, per cui il numero dei *software* considerabili *medical device* è sensibilmente aumentato e ai sensi dell’art. 22 i *device* sono suddivisi in 4 classi di rischio: I, IIA, IIB, III in relazione alla destinazione d’uso e ai rischi che ne derivano. Questa classificazione è effettuata dal fabbricante secondo i criteri dell’Allegato VIII, ma mentre per i dispositivi di classe I è sufficiente una valutazione della conformità e l’apposizione del marchio CE, per i dispositivi appartenenti alle altre classi occorre un controllo più rigoroso da parte dell’Organismo Notificato come definito e disciplinato dal MDR. Infatti, qualora il dispositivo presenti un rischio alto o medio, la valutazione della conformità coinvolge anche esperti indipendenti nominati dalla Commissione e dagli Stati Membri che forniranno un parere scientifico.

Rispetto ai *software* medicali occorre poi operare una differenziazione, che prescinde dalla connessione con un dispositivo e dall’ubicazione del *software*. Nell’ipotesi in cui i *software* vengano utilizzati nel contesto sanitario, ma perseguano esclusivamente finalità generali, essi non sono considerati come dispositivi medici. Qualora, invece, tali *software* forniscano informazioni che possono essere impiegate per assumere decisioni a fini diagnostici o terapeutici ovvero qualora modifichino i dati ricevuti per fornire informazioni mediche nuove e diverse, essi vengono considerati *medical device*; si parla a tal proposito di *Software As Medical Device* (SAMD). Essi sono considerati a medio o ad alto rischio.

In particolare, mentre i *software* medicali realizzati secondo le regole di classificazione della Direttiva 93/42/CEE erano per la maggior parte in classe I (quindi non sottoposti all’obbligo di controllo dell’Organismo Notificato), ai sensi del MDR gli stessi *software* “passano” in larga misura nelle classi IIA e IIB, per le quali è necessario il controllo da parte dell’Organismo Notificato.

Tuttavia, per consentire agli Organismi Notificati *ex* MDR di prepararsi in maniera adeguata ad effettuare le necessarie valutazioni, è stata introdotta una deroga che consente, a certe condizioni, la permanenza dei dispositivi in classe I fino al 26 maggio 2024.

Tanto è stato previsto dal **Regolamento (UE) 2020/561** del Parlamento europeo e del Consiglio del 23 aprile 2020 che è intervenuto a modificare il MDR per quanto riguarda le date di applicazione di alcune delle sue disposizioni. Più precisamente, per quanto riguarda la classificazione in commento, il Regolamento (UE) 2020/561 ha sostituito il primo comma del paragrafo 3 dell’art. 120 del MDR con la seguente disposizione: “*In deroga all’articolo 5 del presente regolamento, un dispositivo di classe I ai sensi della direttiva 93/42/CEE, per il quale è stata redatta una dichiarazione di conformità prima del 26 maggio 2021 e per il quale la procedura di valutazione della conformità ai sensi del presente regolamento richiede il coinvolgimento di un organismo notificato, o un dispositivo con un certificato rilasciato ai sensi della direttiva 90/385/CE o della direttiva 93/42/CEE e valido in virtù del paragrafo 2 del presente articolo, può essere immesso sul mercato o messo in servizio fino*

al 26 maggio 2024, a condizione che a decorrere dal 26 maggio 2021 continui a essere conforme a una di tali direttive, e a condizione che non vi siano cambiamenti significativi nella progettazione e nella destinazione d'uso. Tuttavia, le prescrizioni del presente regolamento in materia di sorveglianza post-commercializzazione, sorveglianza del mercato, vigilanza, registrazione di operatori economici e dispositivi si applicano e sostituiscono le corrispondenti prescrizioni di cui a dette direttive.”.

Tale disposizione propone la questione di cosa debba intendersi con “cambiamenti significativi nella progettazione e nella destinazione d'uso”, in costanza dei quali la medesima disposizione prevede che l'agevolazione cessi di operare.

Anche la commercializzazione del prodotto assume una rinnovata rilevanza, essendo sancito un obbligo di controllo nella fase successiva alla commercializzazione esteso a tutti i soggetti della filiera produttiva: fabbricante, importatore, distributore. Questa nuova ottica riguarderà anche le strutture sanitarie che realizzano autonomamente i propri *medical device*, in quanto, sebbene tali prodotti non siano soggetti alla commercializzazione e non richiedano quindi l'applicazione del marchio CE, sono in ogni caso sottoposti alle regole previste dal MDR; pertanto, anche le strutture sanitarie sono considerate fabbricanti.

Un aspetto particolarmente attuale – vista la pandemia in corso – concerne i *software* che erogano servizi di telemedicina, in quanto possono essere considerati dispositivi medici, specialmente quando prevedono l'elaborazione di dati personali; in questo caso, si pone anche un problema di coordinamento con i principi sanciti dal GDPR.

L'impianto del MDR comporta una serie di adempimenti obbligatori per le imprese, le quali dovranno valutare: il rispetto dei requisiti; l'eventuale cambio di classe di rischio da parte del *device*; la valutazione clinica del dispositivo. Si tratta di attività cruciali, che comportano evidenti costi di *compliance*. Il settore Medtech si caratterizza così per una vera e propria catena di soggetti coinvolti: il produttore del *device*, il programmatore dell'algoritmo, il *trainer*, l'ente sanitario che lo impiega, ma anche, come visto, i soggetti coinvolti nella commercializzazione; si pongono dunque notevoli problemi in tema di responsabilità, sui quali viene da più parti auspicato un apposito intervento del Legislatore.

SUSANNA SANDULLI

[https://www.salute.gov.it/portale/news/p3\\_2\\_1\\_1\\_1.jsp?lingua=italiano&menu=notizie&p=dalministero&id=5499](https://www.salute.gov.it/portale/news/p3_2_1_1_1.jsp?lingua=italiano&menu=notizie&p=dalministero&id=5499)

2021/4(12)BC

### **La legge dello Stato del Wyoming sulle Decentralized Assets Organizations (DAOs) del 21 aprile 2021**

Lo Stato del Wyoming (USA) ha promulgato, il 21 aprile 2021, la legge nota come *Wyoming Decentralized Autonomous Organization Supplement* (“**WDAOS**”) entrata in vigore il 1° luglio 2021.

La WDAOS ha introdotto una disciplina delle *Decentralized Autonomous Organizations* (“**DAO**”) che, nell'attuale panorama legislativo globale, costituisce il primo intervento legislativo volto a disciplinare tale fenomeno. La WDAOS non si è spinta sino a regolare in modo dettagliato le DAO e i rapporti giuridici che da essa possono originarsi. La WDAOS ha, in effetti, adottato un'altra tecnica e ha ricondotto le DAO alla preesistente legislazione societaria, seppure con interessanti peculiarità che - anche in prospettiva sistematica - potranno costituire il fondamento di successive riflessioni.

Prima di illustrare i punti essenziali della WDAOS, si riassumono qui di seguito gli elementi identificativi comunemente associati alle DAO.

La DAO, nella sua essenza fenomenica, è una comunità digitale organizzata e composta da più soggetti.

Dopo la costituzione, la DAO viene promossa dai suoi fondatori: il primo passo successivo alla costituzione consiste, di norma, nel collocamento presso il pubblico dei *token* basati su *blockchain*. Può anche accadere che una DAO sia costituita senza alcun collocamento dei *token* e che i fondatori siano, da subito, gli stessi acquirenti di tutti i *token* emessi.

Tali *token* incorporano normalmente sia il diritto di esser riconosciuti come membri della DAO, sia gli ulteriori diritti - partecipativi e di *governance* - che di volta in volta possono venire in rilievo nel momento di proporre o adottare le deliberazioni che riguardano la DAO e il suo patrimonio.

Di solito, i fondi che costituiscono la dotazione patrimoniale iniziale della DAO sono rappresentati da criptovalute; tale dotazione patrimoniale può variare, nel corso del tempo, in conseguenza di acquisti effettuati dalla DAO con il proprio patrimonio o per effetto di successivi incrementi patrimoniali tramite emissione di nuovi *token* o apporti di altra natura.

La DAO si basa su *smart contract* e su tecnologia *blockchain* e funziona tramite algoritmi decisori, dai contenuti più o meno complessi, che consentono di evitare - in tutto o in parte - l'intervento umano in fase gestoria ed esecutiva.

La DAO è uno strumento che può essere impiegato per un ampio spettro di finalità: attività di investimento; finalità filantropiche; acquisto e rivendita di opere d'arte digitali (come gli NFT); sottoscrizione in comune di abbonamenti a *software* etc.

Le regole di *governance* della DAO sono cristallizzate ed eseguite tramite la *blockchain*, assicurando in tal modo la immodificabilità delle regole di funzionamento; a differenza delle forme tradizionali di associazione tra più soggetti, una DAO opera su un ecosistema digitale che - almeno in parte può funzionare in assenza di un organo a cui sarebbe altrimenti delegata l'amministrazione dell'ente e del suo patrimonio.

Ne discende che la DAO è:

- i. Decentralizzata: perché non è amministrata né gestita da un organo societario/aziendale centrale (ad es. un consiglio di amministrazione, un asset manager, un comitato direttivo etc.) e perché si basa sulla *blockchain*. Le decisioni aventi ad oggetto atti e negozi giuridici che interessano il patrimonio della DAO stessa sono condivise e deliberate dall'intera community di titolari dei token, sulla base di proposte votate senza la presenza di un'autorità centrale.
- ii. Autonoma: perché può eseguire operazioni di rilevanza giuridica (ad es. acquisti, vendite, investimenti etc.) in autonomia e tramite l'esecuzione di algoritmi decisori e *smart contract*, quindi anche in assenza di interventi esterni o di human *governance*;
- iii. Organizzata: perché configura un'organizzazione plurisoggettiva composta dai titolari dei token e che risponde a proprie regole, finalità e obiettivi che sono codificati negli *smart contract* ed eseguite tramite *blockchain*.

Tanto riassunto sul fenomeno socio economico, i punti salienti della disciplina della WDAOS sono i seguenti.

Innanzitutto, la WDAOS ha definito la DAO come una Limited Liability Company ("LLC") i cui articoli dello statuto devono contenere una dichiarazione (*statement*) in base alla quale viene reso noto al pubblico che la società è una DAO (§ 17-31-104, a). In sostanza, la legge del Wyoming non è intervenuta per definire e regolare a tutto tondo il fenomeno delle DAO, ma si è limitata a prevedere che una DAO può adottare il tipo societario previsto per le LLC, seppure con certe caratteristiche proprie che, di fatto, pongono le DAO e le LLC in un rapporto di *species a genus*.

Dato che, ai sensi della WDAOS, le DAO sono innanzi tutto delle LLC, la legge introduce alcune alternative statutarie tipiche per le DAO: lo statuto della DAO/LLC può prevedere, alternativamente, che la DAO sia una LLC gestita dai membri dell'organizzazione (*member managed DAO*), oppure che la gestione sia affidata a un algoritmo (*algorithmically managed DAO*). Se lo statuto non contenesse alcuna indicazione specifica circa la forma di amministrazione, si presume che la DAO/LLC sia una *member managed DAO* (§ 17-31-104, e).

La WDAOS non contiene una definizione di *algorithmically managed DAO*. Pur in assenza di tale definizione di amministrazione algoritmica (che sarebbe stata certamente utile in prospettiva sistematica e comparativa), una LCC/DAO può essere costituita e registrata in base alle leggi del Wyoming solo a condizione che lo *smart contract* su cui si basa il sistema di amministrazione algoritmica consenta l'aggiornamento e la modifica (§ 17-31-104, d). Questa prescrizione lascia intendere che, anche laddove l'amministrazione di una DAO/LLC sia affidata a sistemi algoritmici, potrebbe non esser esclusa la responsabilità "umana" (ad es. in capo ai fondatori) per *culpa in vigilando*, ad esempio in caso di omesso aggiornamento dell'algoritmo decisionale.

La WDAOS precisa ulteriormente che la gestione di una DAO /LLC spetta ai suoi membri in caso di *member managed DAO*; invece, in caso di *algorithmically managed DAO*, in mancanza di diverse prescrizioni statutarie, la gestione spetta direttamente allo *smart contract* che implementa l'algoritmo (§ 17-31-109). Si introduce, in questo modo, la figura dello *smart contract* amministratore di società (con tutte le conseguenti difficoltà e incertezze, sul piano sistematico, che potrebbero conseguire da tale sovrapposizione tra *smart contract* e organo preposto alla gestione della società).

Altre prescrizioni degne di nota contenute nella WDAOS sono le seguenti:

- i. una DAO/LLC deve avere un domiciliatario preposto alla ricezione e notifica di atti giudiziari nello Stato del Wyoming (§ 17-31-104, d);
- ii. la denominazione della LLC deve includere uno dei seguenti termini "DAO", "LAO" (acronimo per *Limited Liability Autonomous Organization* ma sostanzialmente sinonimo di DAO) o "DAO LLC" (§ 17-31-104, e).
- iii. lo statuto della DAO/LLC, oltre a dover dichiarare (v. supra) che la LLC è una DAO, deve contenere il seguente disclaimer (§ 17-31-104, c): "*I diritti dei membri di un'organizzazione autonoma decentralizzata possono differire sostanzialmente dai diritti dei membri di altre LLC. Il Wyoming Decentralized Autonomous Organization Supplement, gli smart contract su cui si fonda la DAO, gli articoli dello statuto [...] possono definire, ridurre o eliminare i doveri delle parti e possono limitare il trasferimento della proprietà dei titoli, il recesso o l'uscita dalla DAO, nonché la restituzione dei conferimenti e lo scioglimento dell'organizzazione autonoma decentralizzata*".
- iv. per quanto concerne la costituzione della DAO/LLC, è previsto che qualsiasi persona possa costituire una DAO e, inoltre, che la DAO può avere uno o più soci al momento della costituzione. Il soggetto che costituisce la DAO non deve necessariamente esser socio stessa, con il che si riconosce la figura del *founder* esterno all'organizzazione (§ 17-31-105, a).
- v. lo statuto della DAO/LLC deve contenere, tra le altre cose, clausole che regolino:
  - a) i rapporti tra i soci e tra questi e la DAO/LLC;
  - b) i diritti e gli obblighi dei partecipanti alla DAO/LLC;
  - c) l'oggetto sociale della DAO/LLC e le modalità di perseguimento del medesimo;
  - d) il diritto di voto e le modalità per il suo esercizio;
  - e) il trasferimento dei diritti di partecipazione nella DAO/LLC;
  - f) il recesso dalla DAO/LLC;

- g) i criteri di liquidazione e ripartizione tra i soci del patrimonio della DAO/LLC in caso di scioglimento;
  - h) le modifiche allo statuto;
  - i) le procedure per la modifica, l'aggiornamento, la modifica o la modifica degli *smart contract*.
- vi. la DAO/LLC è soggetta a scioglimento e liquidazione automatica se, nel corso di un anno, non approva alcuna proposta sottoposta a votazione dai membri (§ 17-31-114, a, iv).

La WDAOS, infine, sembra attribuire massima importanza gerarchica al principio della libertà contrattuale a scapito dei principi generali societari: in base alla WDAOS, infatti, i soci di una DAO/LLC devono osservare, nei rapporti interni tra soci e con la DAO/LLC, soltanto i principi generali di buona fede e correttezza contrattuali, mentre nella DAO/LLC non trovano applicazione i *fiduciary duties* tipici delle normali LLC (§ 17-31-110).

BENEDETTO COLOSIMO

<https://www.wyoleg.gov/Legislation/2021/SF0038>

2021/4(13)CM

### **La prima legge sulla protezione delle informazioni personali della Repubblica Popolare Cinese (la 'PIPL')**

Il 20 agosto 2021, dopo la discussione di due bozze, di cui la prima risalente a ottobre 2020 (su cui v. notizia [2020/4\(4\)CM](#)) e la seconda ad aprile 2021, l'Assemblea Nazionale Popolare della Repubblica popolare cinese ha approvato la 'Legge sulla protezione delle informazioni personali della Repubblica popolare cinese' (中华人民共和国个人信息保护法, *geren xinxi baohu fa*: di seguito "PIPL" dal suo acronimo già affermato in ambito internazionale).

La PIPL è la prima legge cinese interamente ed esclusivamente dedicata alla tutela delle informazioni personali e costituirà, assieme alla Legge sulla sicurezza cibernetica (2017) e alla Legge sulla sicurezza dei dati (2021), il sistema normativo cinese in materia di ICT.

Dopo aver chiarito in premessa il suo scopo, la PIPL circoscrive il suo ambito di applicazione a tutte quelle attività di trattamento delle informazioni personali compiute da organizzazioni e individui nell'esercizio della propria attività d'impresa.

La PIPL disciplina non solo il trattamento delle informazioni personali all'interno della Repubblica Popolare ma anche quelli al di fuori del territorio cinese, in determinati casi (quando il trattamento è necessario per la fornitura di prodotti o servizi a persone fisiche che si trovano all'interno del territorio cinese; quando è necessario per la valutazione o l'analisi del comportamento delle persone fisiche all'interno del territorio cinese; negli altri casi previsti dalla legge o dai regolamenti amministrativi).

Le informazioni personali sono definite, analogamente alla normativa europea in materia, come quelle 'informazioni relative a persone fisiche identificate o identificabili', ad eccezione delle informazioni rese in forma anonima.

La nuova legge pone obblighi in capo ai 'gestori delle informazioni personali' (figura analoga al 'titolare del trattamento' in ambito europeo), definiti come 'le organizzazioni o gli individui che determinano in modo indipendente lo scopo e il metodo del trattamento'.

Tra i principi fondamentali posti dalla legge si evidenziano: il principio di liceità, di necessità e di buona fede del trattamento, il quale non deve essere mai fuorviante, fraudolento, o coercitivo, e che deve essere sempre limitato alle informazioni strettamente necessarie per lo scopo preposto; lo scopo, a sua volta, deve essere chiaramente individuato e ragionevole (vale a dire che il trattamento delle informazioni deve essere direttamente correlato a uno scopo legittimo e la raccolta di tali informazioni deve limitarsi alle sole informazioni la cui acquisizione è necessaria al perseguimento di tale scopo); la trasparenza è richiesta in termini di regole, finalità, metodo e ambito del trattamento; l'accuratezza, secondo cui la raccolta e la conservazione delle informazioni deve essere sempre accurata, completa e aggiornata; infine, la sicurezza, per cui i gestori di informazioni personali devono garantire e adottare tutte le misure necessarie per salvaguardare la sicurezza di tutte le informazioni personali elaborate.

La PIPL prevede, affinché si possano trattare informazioni personali, che alcune condizioni debbano essere soddisfatte. In particolare: deve essere fornito un consenso chiaro ed espresso della persona interessata dal trattamento; tale consenso deve essere dato su base volontaria e previa rappresentazione di tutte le modalità del trattamento; il consenso può essere revocato in qualsiasi momento dalla persona interessata e il titolare del trattamento deve predisporre una modalità di revoca del consenso che sia facilmente accessibile al soggetto i cui dati sono trattati; inoltre, il responsabile del trattamento non può rifiutarsi di fornire prodotti o servizi a chi non ha prestato il proprio consenso, a meno che il trattamento dei dati personali non sia necessario per la fornitura dei suddetti prodotti o servizi.

Con riferimento alle 'informazioni personali sensibili' il PIPL offre un livello di protezione superiore rispetto alle generiche informazioni personali. Le tipologie di dati rientranti in questa categoria sono: i dati biometrici, gli orientamenti religiosi, le informazioni relative allo stato di salute delle persone, le informazioni relative allo stato patrimoniale delle persone e i dati personali dei soggetti minori di 14 anni. Affinché tali informazioni possano essere trattate occorre un consenso rafforzato oltre che una finalità specifica, necessaria e legittima.

CORRADO MORICONI 马思勇

Link al testo originale in cinese della Legge sul sito dell'Assemblea Nazionale del Popolo:  
<http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>

# ANNO 2022

## [2022/1\(1\)EB](#)

L'attuazione della direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (D.Lgs. 8 novembre 2021, n. 177) ..... p. 149

## [2022/1\(2\)RA](#)

L'attuazione della direttiva "Open Data" (UE) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (D.Lgs. 8 novembre 2021, n. 200, modificativo del D.Lgs. 36/2006) ..... p. 152

## [2022/1\(3\)EMI](#)

L'attuazione della direttiva (UE) 2018/1972 che istituisce il Codice europeo delle comunicazioni elettroniche (D.Lgs. 8 novembre 2021, n. 207, modificativo del D. Lgs. 259/2003) ..... p. 155

## [2022/1\(4\)SO](#)

Verso il Data Act: la proposta di Regolamento del Parlamento e del Consiglio su regole armonizzate sull'accesso equo e l'uso dei dati (legge sui dati) COM(2022) 68 final del 23 febbraio 2022 ..... p. 156

## [2022/1\(5\)ST](#)

La proposta di Dichiarazione europea sui diritti e i principi digitali per il decennio digitale COM(2022) 28 final del 26 gennaio 2022 ..... p. 160

## [2022/1\(6\)SO](#)

La proposta di Regolamento del Parlamento e del Consiglio relativo alla trasparenza e al targeting della pubblicità politica COM(2021) 731 final del 25 novembre 2021 ..... p. 163

## [2022/1\(7\)ES](#)

Il Decreto del Ministero dell'economia e delle finanze del 13 gennaio 2022 sull'iscrizione alla sezione speciale del registro dei cambiavalute da parte dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale ..... p. 165

## [2022/1\(8\)GDI](#)

La decisione del 10 febbraio 2022 del Garante privacy italiano sul trattamento di dati biometrici da parte di Clearview AI ..... p. 167

## [2022/1\(9\)CR](#)

La decisione del 13 gennaio 2022 del Garante privacy austriaco sul trasferimento di dati personali negli USA per Google Analytics ..... p. 168

## [2022/1\(10\)CR](#)

La decisione del 10 febbraio 2022 del Garante privacy francese sul trasferimento di dati personali negli USA per Google Analytics ..... p. 170

## [2022/1\(11\)VR](#)

La decisione del 2 febbraio 2022 del garante privacy belga sul Real Time Bidding e le attività di online advertising a proposito del Quadro di Trasparenza e Consenso elaborato e gestito da IAB Europe ..... p. 171

## [2022/1\(12\)FG](#)

La sentenza della Cassazione n. 3952 del 8 febbraio 2022 sul diritto all'oblio e le copie cache ..... p. 177

[2022/1\(13\)FDA](#)

Le “*Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration*” dello *European Law Institute* (ELI) del 3 marzo 2022 ..... p. 179

[2022/2\(1\)RA](#)

Approvato il ‘Data Governance Act’: Regolamento (UE) 2022/868 del 30 maggio 2022 sulla governance europea dei dati ..... p. 181

[2022/2\(2\)BC](#)

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 ..... p. 187

[2022/2\(3\)AF](#)

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 .. p. 191

[2022/2\(4\)FG](#)

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) ..... p. 192

[2022/2\(5\)SO](#)

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: il documento pubblicato il 28 giugno 2022 dallo *UK Intellectual Property Office* ..... p. 196

[2022/2\(6\)EMI](#)

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) ..... p. 198

[2022/2\(7\)VR](#)

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* ..... p. 200

[2022/2\(8\)ES](#)

Il Parere della BCE del 29 dicembre 2021 sulla proposta di regolamento sull’intelligenza artificiale (*‘Artificial Intelligence Act’*) ..... p. 205

[2022/2\(9\)ES](#)

Il Regolamento di Banca d’Italia del 22 marzo 2022 sul trattamento dei dati personali effettuato nell’ambito della sua gestione degli esposti ..... p. 208

[2022/2\(10\)AAM](#)

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” ..... p. 211

[2022/2\(11\)AF](#)

La proposta di uno ‘*US Stablecoin Trust Act*’ del *U.S. Senate Banking Committee* del 6 aprile 2022 ..... p. 213

<a href="#">2022/2(12)VP</a>	Il Libro Bianco 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) .....	p. 214
<a href="#">2022/3(1)TDMCDV</a>	Verso la AI Liability Directive: la proposta della Commissione europea del 28 settembre 2022 per una direttiva sull'adattamento delle regole di responsabilità civile all'Intelligenza Artificiale .....	p. 217
<a href="#">2022/3(2)TDMCDV</a>	Verso la nuova Product Liability Directive: la proposta della Commissione europea del 28 settembre 2022 per una nuova direttiva sulla responsabilità da prodotto difettoso che abroga la Direttiva 85/374/CEE .....	p. 220
<a href="#">2022/3(3)RA</a>	Proposta di Regolamento riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo ( <i>Data Act</i> ): <i>First Presidency compromise text</i> del 12 luglio 2022 .....	p. 222
<a href="#">2022/3(4)VR</a>	La proposta di Regolamento UE sui requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali (c.d. Cyber Resilience Act) .....	p. 226
<a href="#">2022/3(5)EMI</a>	Verso il regolamento europeo di progettazione eco-sostenibile dei dispositivi mobili tecnologici .....	p. 230
<a href="#">2022/3(6)ES</a>	Gli ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection .....	p. 232
<a href="#">2022/3(7)FG</a>	Il parere congiunto EDPB-EDPS n.4/2022 del 28.7.2022 sulla proposta di regolamento della Commissione Europea del 11.05.2022 che stabilisce norme per prevenire e combattere l'abuso sessuale dei minori .....	p. 237
<a href="#">2022/3(8)CR</a>	NOYB denuncia Google alla CNIL per l'invio di e-mail pubblicitarie non richieste senza consenso degli utenti .....	p. 239
<a href="#">2022/3(9)CR</a>	Il Garante privacy esprime parere negativo sullo schema di decreto sull'Ecosistema Dati Sanitari (parere del 22.8.2022) .....	p. 240
<a href="#">2022/3(10)LC</a>	Accesso ai risultati della ricerca scientifica finanziata con fondi federali: nuove linee guida negli Stati Uniti d'America .....	p. 241
<a href="#">2022/3(11)AF</a>	Le proposte normative dell'11 ottobre 2022 del <i>Financial Stability Board</i> in materia di cripto-attività e <i>global stablecoins</i> .....	p. 243
<a href="#">2022/4(1)ST</a>	Approvato il Digital Services Act (DSA): Regolamento (UE) 2022/2065 del 19.10.2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE .....	p. 245
<a href="#">2022/4(2)VR</a>	Approvato il Digital Markets Act (DMA): Regolamento (UE) 2022/1925 del 14.09.2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive 2019/1937/UE e 2020/1828/UE .....	p. 249

[2022/4\(3\)ES](#)

Approvato il 'DORA': Regolamento (UE) 2022/2554 del 14.12.2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 ..... p. 253

[2022/4\(4\)SO](#)

Le modifiche apportate alla disciplina dell'abuso di dipendenza economica di cui alla legge sulla subfornitura, con decorrenza dal 31 ottobre 2022 ..... p. 256

[2022/4\(5\)RA](#)

La EU Interinstitutional declaration on digital rights and principles del 14.11.2022 ..... p. 257

[2022/4\(6\)DI](#)

Il codice deontologico "rafforzato" del 2022 di buone pratiche contro la disinformazione ..... p. 259

[2022/4\(7\)ST](#)

NetChoice LLC v. Paxton , n. 21-51178- United States Court of Appeals for the Fifth Circuit, provvedimento del 16.9.2022: libertà di parola *versus* moderazione di contenuti da parte delle piattaforme *online* ..... p. 261

[2022/4\(8\)CR](#)

La sentenza CGUE del 20.10.2022 nella causa C 77/21 sui principi di limitazione delle finalità e di limitazione della conservazione ex art. 5 lett. b) ed e) GDPR ..... p. 263

[2022/4\(9\)CAT](#)

La sentenza CGUE del 27.10.2022 nella causa C-129/21 Proximus (Annuaire électronique publics) sulle misure da adottarsi da parte del titolare del trattamento di dati personali per informare i motori di ricerca in Internet di una richiesta di cancellazione rivoltagli dall'interessato ..... p. 265

[2022/4\(10\)FDA](#)

Verso l'Interoperable Europe Act: la proposta della Commissione di regolamento europeo sull'interoperabilità nel settore pubblico del 18.11.2022 ..... p. 267

[2022/4\(11\)SO](#)

I comunicati del Garante privacy italiano del 18.10.2022, del 21.10.2022 e del 12.11.2022 di avvio di istruttorie a carico di testate editoriali online per iniziative di *cookie wall* e monetizzazione di dati personali ..... p. 268

[2022/4\(12\)VR](#)

Il comunicato del 14.11.2022 del Garante privacy italiano di avvio di istruttorie per i sistemi di videosorveglianza dei Comuni di Lecce e di Arezzo ..... p. 269

[2022/4\(13\)ES](#)

La sentenza Cassazione Sez. 2 Penale n. 44378/2022 del 26.10.2022 sulla qualificazione della moneta virtuale e delle Initial Coin Offerings (a proposito di un sequestro penale preventivo di wallet contenente bitcoin e di una fattispecie di reato di abusivismo finanziario ai sensi dell'art. 166 co. 1 TUF) .. p. 270

[2022/4\(14\)EB](#)

L'Ordinanza della Cassazione Prima Sez. Civile n. 34658/2022 del 24.11.2022 sul diritto all'oblio e l'ordine di rimozione c.d. globale (regime Codice privacy anteriore al GDPR) ..... p. 273

[2022/4\(15\)FDA](#)

La sentenza Tar Campania, sede di Napoli, Sez. III, n. 7003 del 14 novembre 2022 sull'uso di sistemi algoritmici nei procedimenti amministrativi ..... p. 275

[2022/4\(16\)FG](#)

L'ordinanza del Tribunale di Roma del 20.7.2022 su NFT: il caso della Juventus ..... p. 276

[2022/4\(17\)EMI](#)

L'order del 7.11.2022 della District Court of New Hampshire (USA) sulla qualificazione di un utility token come security ..... p. 277

[2022/4\(18\)RMo](#)

L'Assurance of voluntary compliance tra Google e lo Stato della Pennsylvania (USA) del 14.12.2022 sui dati di localizzazione ..... p. 279

[2022/4\(19\)AM-GD](#)

Le due sentenze "gemelle diverse" del Tar Lazio, sede di Roma, Sez. I del 18.11.2022 nei casi riguardanti Apple (sentenza n.15317) e Google (sentenza n.15326) in materia di pratiche commerciali sleali e patrimonializzazione dei dati personali ..... p. 282



**L'attuazione della direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (D.Lgs. 8 novembre 2021, n. 177).**

Il 12 dicembre 2021 è entrato in vigore il Decreto Legislativo 177/2021 del 5 novembre 2021 (il “**Decreto**”), attuativo 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 (la “**Direttiva**”). Il Decreto (emanato dopo il termine prescritto dal legislatore europeo del 7 giugno 2021) è frutto dell'ampia delega conferita al Governo ai fini del recepimento della Direttiva all'interno della legislazione nazionale.

L'obiettivo dichiarato della Direttiva - e dunque del D.Lgs. di adeguamento - è quello di adattare gli strumenti di tutela del diritto d'autore alla modernizzazione generata dall'evoluzione tecnologica ed in particolare da nuove forme di comunicazione, caricamento, condivisione e creazione dei contenuti, le quali costituiscono inedite modalità di riproduzione e “moltiplicazione” dell'opera protetta, che potenzialmente minano l'armonizzazione del diritto d'autore tra gli Stati membri.

In particolare, le disposizioni della Direttiva concernono: l'adeguamento di talune eccezioni e limitazioni all'ambiente digitale e al contesto transfrontaliero (Titolo II); misure volte a facilitare le procedure di concessione delle licenze e a garantire un più ampio accesso ai contenuti (Titolo III), facilitando in particolare, ma non solo, la divulgazione delle opere fuori commercio (Capo I), la concessione di licenze collettive con effetto esteso (Capo II), l'accesso e disponibilità di opere audiovisive su piattaforme di video su richiesta (Capo III), la previsione concernente le opere delle arti visive di dominio pubblico (Capo IV); misure miranti a garantire il buon funzionamento del mercato per il diritto d'autore (Titolo IV), segnatamente la protezione delle pubblicazioni giornalistiche in caso di utilizzo *online* (Capo I), l'utilizzo di contenuti protetti da parte di prestatori di servizi di condivisione di contenuti *online* (Capo II); il principio e le regole di equa remunerazione di autori e artisti (interpreti o esecutori) nei contratti di sfruttamento (Capo III).

Con riguardo alla trasposizione nel diritto interno, il Decreto ha determinato importanti modifiche all'articolato della legge sul diritto d'autore (la l. 633/1941, “**l.a.**”), introducendo anche alcuni correttivi che in certi casi potrebbero apparire estranei alle intenzioni del legislatore europeo.

Con riferimento al contenuto del Titolo II della Direttiva, sono state introdotte nella l.a. nuove eccezioni e limitazioni ai fini di adeguamento ai nuovi mezzi e conseguente utilizzo di materiale protetto in ambiente digitale nei settori dell'istruzione, della ricerca e della conservazione del patrimonio culturale. In particolare, è stato introdotto l'articolo 70-*bis* l.a. che legittima taluni utilizzi di brani, parti di opere o altri materiali per attività svolte con mezzi digitali ed esclusivamente per finalità illustrative ad uso didattico. All'articolo 68 l.a. è aggiunto il comma 2-*bis* che legittima “sempre” l'eccezione al diritto di riproduzione e di realizzazione di copie di opere protette da parte degli istituti di tutela del patrimonio culturale per finalità di conservazione di tali opere. Simili eccezioni sono state pure introdotte con riferimento alle attività di *Text and Data mining* (TDM) agli articoli 70-*ter* e 70-*quater* l.a. Il TDM, in italiano ‘estrazione di testo e di dati’, è definito come “*qualsiasi tecnica automatizzata volta ad analizzare grandi quantità di testi, suoni, immagini, dati o metadati in formato digitale con lo scopo di generare informazioni, inclusi modelli, tendenze e correlazioni?*” (art. 70-*ter*, co. 2 l.a.). Ai sensi dell'art. 70-*ter* co. 1 l.a., “[s]ono consentite le riproduzioni compiute da organismi di ricerca e da istituti di tutela

*del patrimonio culturale, per scopi di ricerca scientifica, ai fini dell'estrazione di testo e di dati da opere o da altri materiali disponibili in reti o banche di dati cui essi hanno lecitamente accesso, nonché la comunicazione al pubblico degli esiti della ricerca ove espressi in nuove opere originali*". Per 'istituti di tutela del patrimonio culturale' si intendono "le biblioteche, i musei, gli archivi, purché aperti al pubblico o accessibili al pubblico, inclusi quelli afferenti agli istituti di istruzione, agli organismi di ricerca e agli organismi di radiodiffusione pubblici, nonché gli istituti per la tutela del patrimonio cinematografico e sonoro e gli organismi di radiodiffusione pubblici" (art. 70-ter co. 3 l.a.), mentre per 'organismi di ricerca' si intendono "le università, comprese le relative biblioteche, gli istituti di ricerca o qualsiasi altra entità il cui obiettivo primario è quello di condurre attività di ricerca scientifica o di svolgere attività didattiche che includano la ricerca scientifica, che alternativamente:

a) operino senza scopo di lucro o il cui statuto prevede il reinvestimento degli utili nelle attività di ricerca scientifica, anche in forma di partenariato pubblico-privato;

b) perseguano una finalità di interesse pubblico riconosciuta da uno Stato membro dell'Unione europea", mentre non si considerano organismi di ricerca "quelli sui quali è esercitata da imprese commerciali un'influenza determinante tale da consentire un accesso su base preferenziale ai risultati generati dalle attività di ricerca scientifica" (art. 70-ter commi 4 e 5 l.a.).

Fuori dalla suddetta eccezione, dichiaratamente intesa a favorire gli scopi di ricerca scientifica perseguiti dai suddetti soggetti, la disciplina è disegnata dall'art. 70-*quater* l.a. in modo tale da dipendere sostanzialmente dalla volontà dei titolari del diritto d'autore e dei diritti connessi nonché dai titolari delle banche dati. Ed infatti, ai sensi dell'art. 70-*quater* l.a., fuori dai casi dell'eccezione appena riferita, disciplinata dall'art. 70-*ter*, "sono consentite le riproduzioni e le estrazioni da opere o da altri materiali contenuti in reti o in banche di dati cui si ha legittimamente accesso ai fini dell'estrazione di testo e di dati", ma si soggiunge subito appresso che "[l]'estrazione di testo e di dati è consentita quando l'utilizzo delle opere e degli altri materiali non è stato espressamente riservato dai titolari del diritto d'autore e dei diritti connessi nonché dai titolari delle banche dati". Numerose perplessità hanno accompagnato le previsioni della Direttiva in relazione all'effettiva portata del diritto di riproduzione e alla sua applicazione nel contesto di attività di TDM, così come in relazione alle nozioni di 'testo', 'dati' ed 'informazioni', non definiti nella Direttiva (e nemmeno nel Decreto), nonché in relazione recepimento nazionale, che, per certi aspetti, sembra essere anche più restrittivo della disciplina della Direttiva nel configurare l'ambito delle eccezioni e delle limitazioni. Si tratta comunque di una novità che ha una sicura importanza nel disegnare il rapporto tra diritti esclusivi e uso automatizzato delle opere.

Il Decreto, inoltre, interviene introducendo nella l.a. un nuovo Titolo II-*quinques*, a sostegno degli istituti di tutela del patrimonio culturale nella digitalizzazione e diffusione, anche transfrontaliera, delle opere e di altri materiali fuori commercio inserendo gli artt. da 102-*undecies* a 102-*septiesdecies* l.a., che dettano: la definizione di 'opere e di altri materiali fuori commercio' e le procedure per individuare ulteriori elementi per la definizione di opere fuori commercio; la gestione delle licenze collettive estese e l'applicazione dell'eccezione specifica; la risoluzione dei conflitti concernenti la disciplina delle opere orfane; la regolamentazione delle misure di pubblicità. Lo sfruttamento delle opere fuori commercio può avvenire solo ove l'istituto di tutela del patrimonio culturale (come definito dall'art. 70-*ter* l.a.), accertata la natura di opera o materiale fuori commercio, abbia richiesto all'organismo di gestione collettiva di cui al D.Lgs. 35/2017, rappresentativo dei titolari dei diritti per tipologia di opera o di diritto oggetto della licenza, il rilascio di una licenza a fini non commerciali per la riproduzione, la distribuzione, la comunicazione o la messa a disposizione al pubblico dell'opera.

Qualora il titolare dei diritti non abbia conferito mandato ad alcun organismo di gestione collettiva, la competenza al rilascio della licenza spetterà all'organismo che a livello nazionale

sia sufficientemente rappresentativo dei titolari dei diritti, ovvero ai tre organismi maggiormente rappresentativi. Inoltre, i titolari dei diritti, ai sensi dell'art. 102-*quaterdecies* l.a., possono sempre ottenere l'esclusione delle loro opere dall'applicazione delle licenze collettive estese.

Uno degli articoli che in sede di recepimento ha fatto più discutere è l'articolo 14 della Direttiva, che liberalizza la riproduzione delle opere delle arti visive ormai cadute in pubblico dominio. La norma deriva dalla necessità di risolvere la specifica esigenza di dare effettività al pubblico dominio, liberalizzando le riproduzioni fotografiche che non abbiano carattere creativo, sorta in seguito ad una recente pronuncia della Corte di Giustizia Federale tedesca. La disposizione ha destato interrogativi con riguardo alle possibili modalità della sua trasposizione nel nostro ordinamento, alla luce del fatto che essa si pone in conflitto con la disciplina autorale della fotografia semplice (art. 87 l.a.) ed ancor di più con quanto disposto dal Codice dei beni culturali e del paesaggio (D.lgs. 22 gennaio 2004, n. 42, c.d. Codice Urbani), che sottopone ad una concessione la riproduzione di beni culturali per scopi commerciali (art. 108 Codice dei beni culturali e del paesaggio). Da parte dei sostenitori dell'*open access* alla cultura non erano mancate dichiarazioni di soddisfazione per l'intravista possibilità di una piena liberalizzazione della riproduzione del patrimonio culturale, che sarebbe seguita al recepimento della norma in questione, compresa la possibilità di realizzazione della c.d. libertà di panorama. Questa norma è oggi stata trasfusa nel nuovo articolo 32-*quater* l.a., che però, per un verso, si limita a recepire letteralmente il testo europeo, non consentendo di chiarire il rapporto con la disciplina nazionale della fotografia semplice, dall'altro fa espressamente salvo il regime del Codice dei beni culturali e del paesaggio: "*Alla scadenza della durata di protezione di un'opera delle arti visive, anche come individuate all'articolo 2, il materiale derivante da un atto di riproduzione di tale opera non è soggetto al diritto d'autore o a diritti connessi, salvo che costituisca un'opera originale. Restano ferme le disposizioni in materia di riproduzione dei beni culturali di cui al decreto legislativo 22 gennaio 2004, n. 42*". La norma lascia integralmente in vigore le disposizioni confliggenti previste dal Codice Urbani, mancando così l'occasione di realizzare le intenzioni della Direttiva

Acceso è stato pure il dibattito antecedente al recepimento del successivo art. 15 della Direttiva, che introduce nell'*acquis* unionale un nuovo diritto connesso in favore degli editori *online*. L'intervento ha lo scopo di disciplinare il tema dell'utilizzo *online* dei contributi editoriali da parte dei prestatori di servizi della società dell'informazione come fenomeno potenzialmente lesivo del diritto d'autore. Il legislatore ha dunque previsto per gli editori un diritto connesso a quello dell'autore per la riproduzione e la messa a disposizione del pubblico di pubblicazioni di carattere giornalistico, sottoponendo la condivisione *online* degli stessi da parte dei prestatori dei servizi, ad una autorizzazione da parte dell'editore.

Non sono coperti da tale diritto connesso i collegamenti ipertestuali, le singole parole e gli estratti molto brevi; sono inoltre liberi gli utilizzi privati e non commerciali dell'opera in questione. L'articolo è stato recepito in sede nazionale agli artt. 43-*bis* e 70-*quinquies* l.a. È però presente, nel testo di recepimento una importante precisazione tutta italiana in relazione alla definizione di "*estratto molto breve di pubblicazione di carattere giornalistico*", per tale intendendosi una "*qualsiasi porzione di tale pubblicazione che non dispensi [il lettore] dalla necessità di consultazione dell'articolo giornalistico nella sua integrità*" (art. 43-*bis* co. 7 l.a.).

Le norme, in ossequio a quanto traspongono, riconoscono il diritto agli autori e agli editori ad una remunerazione. Tuttavia, la formulazione dell'obbligo, introdotto dal comma 8 dell'articolo 43-*bis* l.a., per i prestatori di servizi di corrispondere un "*equo compenso*" agli editori, ha fatto dubitare della sua conformità alla Direttiva e, sul piano nazionale, del rispetto dei limiti di cui alla legge delega che ha incaricato il Governo, per la circostanza che tale previsione sembra trasformare il diritto esclusivo degli editori a una sorta di diritto a un equo

compenso. Il medesimo comma prevede anche che entro 60 giorni dall'entrata in vigore del Decreto l'AGCOM adotti un regolamento che individui i criteri per la determinazione del compenso. Proprio su questa ultima previsione, l'AGCM – in un più ampio parere sull'attuazione della Direttiva, espresso nell'adunanza del 31 agosto 2021 (<https://www.agcm.it/dotcmsdoc/bollettini/2021/38-21.pdf>) – si era espressa contrariamente, ritenendo l'intervento dell'autorità pubblica ingiustificatamente limitativo della libertà contrattuale degli operatori economici. L'AGCM aveva pertanto suggerito di demandare il compito di intermediazione agli organismi di gestione collettiva e alle entità di gestione indipendenti, ma il legislatore italiano non ha accolto il suggerimento.

Infine, l'articolo 17 della Direttiva, trasposto nel Titolo II- *quater* l.a., contiene il riconoscimento che, come sostenuto da tempo dalla giurisprudenza, i prestatori di servizi di condivisione di contenuti *online* effettuano un atto di comunicazione al pubblico o di messa a disposizione del pubblico in relazione agli atti di caricamento di materiali o di opere protette effettuato dai loro utenti (c.d. *user generated content*). Per questi atti non si applica il regime di esonero di responsabilità già previsto dalla Direttiva 2000/31/CE (c.d. direttiva sul commercio elettronico), con la conseguenza che, in assenza di una valida autorizzazione, i prestatori di servizi di condivisione di contenuti *online* devono porre in essere una serie di specifiche attività (*best efforts*) volte a garantire i diritti esclusivi degli autori, altrimenti incorrendo in responsabilità. A tale regime sono però affiancate delle eccezioni e delle fattispecie di esenzione parziale da responsabilità per certe tipologie di ISP. Di particolare interesse è il recepimento all'articolo 102-*decies* l.a. del procedimento di reclamo e ricorso, previsto dal comma 9 dell'art. 17 della Direttiva. Interessante segnalare che, come previsto dalla Direttiva, anche l'art. 102-*decies* l.a. prevede che le decisioni sulla richiesta di disabilitazione o la rimozione dei contenuti debbano essere soggette a “*verifica umana*”. In più, però, il nostro legislatore ha scelto, in assenza di una simile disposizione della Direttiva, di disabilitare i contenuti fino al termine della procedura di reclamo, tutelando così maggiormente il titolare dei diritti (art. 102-*decies*, co. 3 l.a.: “*Nelle more della decisione sul reclamo, i contenuti in contestazione rimangono disabilitati.*”). Inoltre si evidenzia che la gestione dei ricorsi è stata attribuita alla competenza di AGCOM che dovrà, entro 60 giorni dall'entrata in vigore del Decreto in argomento, emanare un regolamento *ad hoc*. È tuttavia precisato che è impregiudicato il diritto di ricorrere all'autorità giudiziaria (art. 102-*decies*, co. 4 l.a.).

In conclusione, è possibile ritenere che il Decreto introduca delle importanti novità alla disciplina del diritto d'autore, la cui concreta portata si coglierà nel prossimo futuro.

EMANUELA BURGIO

<https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2021-11-08;177>

2022/1(2)RA

**L'attuazione della direttiva “Open Data” (UE) 2019/1024, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (D.Lgs. 8 novembre 2021, n. 200, modificativo del D.Lgs. 36/2006)**

Il 15 dicembre 2021 è entrato in vigore il D.Lgs. 8 novembre 2021, n. 200, recante le disposizioni di attuazione, nell'ordinamento italiano, della direttiva (UE) 2019/1024 del 20 giugno 2019, “*relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico*” (c.d.

direttiva *Open Data*), che ha abrogato la direttiva 2003/98/CE, “*relativa al riutilizzo dell’informazione del settore pubblico*”.

La direttiva *Open Data* detta standard ‘minimi’ sul riutilizzo dei documenti – nella disponibilità di enti pubblici e di imprese pubbliche e private degli Stati Membri – contenenti dati pubblici, al fine di promuovere l’utilizzo dei ‘dati aperti’ e di incentivare la ricerca e l’innovazione. E l’art. 1 del D.Lgs. n. 200/2021, che a tale direttiva ha dato attuazione, ha recato importanti modifiche al D.Lgs. 24 gennaio 2006, n. 36, che aveva a propria volta recepito la direttiva 2003/98/CE. Ai sensi del D.Lgs. 36/2006, ‘dato pubblico’ è il “dato conoscibile da chiunque” e ‘documento’ è, secondo la definizione del medesimo Decreto Legislativo, come integrato dal D. Lgs. 200/2021, “la rappresentazione di atti, fatti e dati a prescindere dal supporto, cartaceo o elettronico, registrazione sonora, visiva o audiovisiva o qualsiasi parte di tale contenuto nella disponibilità della pubblica amministrazione o dell’organismo di diritto pubblico. La definizione di documento non comprende i programmi informatici”.

Si riportano di seguito le principali novità introdotte dal nuovo articolo.

Il comma 2 prevede un’estensione dell’ambito applicativo del D.Lgs. n. 36/2006, tanto sul piano soggettivo che su quello oggettivo. In particolare, esso stabilisce, per un verso, che anche le imprese pubbliche e private sono tenute a rendere disponibili, ai fini del relativo riutilizzo, i documenti contenenti dati pubblici e, per altro verso, che il decreto trova altresì applicazione con riguardo ai ‘dati della ricerca’, agli altri dati nella disponibilità di imprese pubbliche e private che assolvano oneri od obblighi di servizio pubblico ovvero siano, in generale, gestori di servizi pubblici con riguardo ai servizi di pubblico interesse, nonché ai documenti ai quali si applica il D.Lgs. 27 gennaio 2010, n. 32.

Il comma 3 modifica alcune delle definizioni contenute nel decreto del 2006, da un lato, aggiornando riferimenti normativi ormai superati (come nel caso della definizione di ‘pubblica amministrazione’) e, d’altro lato, introducendo nuove definizioni, sulla scia di quanto previsto dalla direttiva: è il caso delle definizioni di ‘anonimizzazione’, ‘dati dinamici’, ‘dati della ricerca’, ‘serie di dati di elevato valore’ e ‘riutilizzo’, che si trovano nelle seguenti nuove lettere dell’art. 2 co. 1 D.Lgs. 36/2006 così formulate:

“*c-quinquies*) anonimizzazione: la procedura mirante a rendere anonimi documenti, rendendoli non riconducibili a una persona fisica identificata o identificabile, ovvero la procedura mirante a rendere anonimi dati personali in modo da impedire o da non consentire più l’identificazione dell’interessato;

*c-sexies*) dati dinamici: documenti informatici, soggetti ad aggiornamenti frequenti o in tempo reale, in particolare a causa della loro volatilità o rapida obsolescenza;

*c-septies*) dati della ricerca: documenti informatici, diversi dalle pubblicazioni scientifiche, raccolti o prodotti nel corso della ricerca scientifica e utilizzati come elementi di prova nel processo di ricerca, o comunemente accettati nella comunità di come necessari per convalidare le conclusioni e i risultati della ricerca;

*c-octies*) serie di dati di elevato valore: documenti il cui riutilizzo è associato a importanti benefici per la società, l’ambiente e l’economia, in considerazione della loro idoneità per la creazione di servizi, applicazioni a valore aggiunto e nuovi posti di lavoro, nonché del numero dei potenziali beneficiari dei servizi e delle applicazioni a valore aggiunto basati su tali serie di dati; [...]

e) riutilizzo: l’uso da parte di persone fisiche o giuridiche di documenti detenuti da:

1) pubbliche amministrazioni o organismi di diritto pubblico, per fini commerciali o per fini non commerciali, diversi da quelli istituzionali per i quali i documenti sono stati prodotti, fatta eccezione per lo scambio di documenti tra pubbliche amministrazioni, o organismi di diritto pubblico, ovvero tra amministrazioni e organismi di diritto pubblico,

posto in essere esclusivamente nell'ambito dell'espletamento dei compiti istituzionali di cui sono titolari;

2) imprese pubbliche e imprese private di cui all'articolo 1, comma 2-*quater*, per fini commerciali o per fini non commerciali, diversi da quelli relativi alla fornitura dei servizi di interesse generale per i quali i documenti sono stati prodotti, fatta eccezione per lo scambio di documenti tra imprese pubbliche e pubbliche amministrazioni o organismi di diritto pubblico posto in essere esclusivamente nell'ambito dell'espletamento dei compiti istituzionali delle pubbliche amministrazioni”.

Il comma 4 introduce poi alcune modifiche alle esclusioni dall'ambito applicativo della disciplina. Tra queste, particolarmente rilevanti appaiono quelle relative ai documenti: (i) detenuti da imprese pubbliche, prodotti al di fuori della prestazione di servizi di interesse generale e/o connessi ad attività direttamente esposte alla concorrenza e non soggette alle norme in materia di appalti; (ii) esclusi dall'accesso procedimentale o dall'accesso civico semplice o generalizzato, ai sensi della normativa vigente; (iii) per i quali l'accesso è escluso, limitato o comunque pregiudizievole per la vita privata o l'integrità delle persone, alla luce delle norme in materia di protezione dei dati personali.

Il comma 6 riscrive integralmente il procedimento relativo all'esame della richiesta di riutilizzo dei documenti racchiuso all'art. 5 del decreto modificato. In particolare, stabilisce un termine di 30 giorni (prorogabile per ulteriori 20, “nel caso in cui le richieste siano numerose o complesse”) ai fini dell'esame delle richieste: in caso di decisione positiva, i documenti sono resi disponibili al richiedente, ove possibile, in forma elettronica e, se necessario, mediante licenza. Avverso l'eventuale provvedimento di diniego, necessariamente motivato, il richiedente può esperire i mezzi di tutela previsti dall'art. 25, comma 4 e 5, della l. n. 241/1990.

Il nuovo art. 6 del D.Lgs. n. 36/2006, introdotto dal comma 7 dell'art. 1 D.Lgs. 36/2006, stabilisce poi che gli enti e le imprese pubbliche debbono mettere a disposizione i propri documenti in formato leggibile meccanicamente e aperto; con particolare riguardo ai dati dinamici e ai dati di elevato valore, i documenti devono essere messi a disposizione tramite adeguata *application programming interface* (API) e, ove possibile, mediante *download* in blocco.

Fermo il principio relativo alla gratuità della messa a disposizione dei dati, il comma 8 fa salva la possibilità per i detentori di richiedere un corrispettivo per il recupero dei costi marginali per le attività svolte a tal fine, nonché per l'anonimizzazione dei dati personali o per proteggere le informazioni commerciali di carattere riservato. Si fa poi rinvio a un decreto del Ministero dell'economia e delle finanze per l'individuazione dell'elenco dei soggetti esclusi dal principio di gratuità.

Il comma 9 novella l'art. 8 del D.Lgs. n. 36/2006, prevedendo l'adozione di licenze standard per il riutilizzo dei dati: si stabilisce, in particolare, che esse non devono subordinare il riutilizzo a condizioni, salvo queste siano obiettive, proporzionate, non discriminatorie e comunque giustificate da un pubblico interesse.

Il comma 11 introduce il nuovo art. 9-*bis* del D.Lgs. n. 36/2006, concernente il riutilizzo dei ‘dati della ricerca’ allorquando essi siano il risultato di attività di ricerca finanziata con fondi pubblici e quando gli stessi dati siano resi pubblici, anche attraverso l'archiviazione in una banca dati pubblica, da ricercatori, organizzazioni che svolgono attività di ricerca e organizzazioni che finanziano la ricerca, tramite una banca dati gestita a livello istituzionale o su base tematica. Esso prevede che tali dati debbano essere riutilizzabili a fini commerciali e no, in conformità a quanto previsto dal decreto e comunque nel rispetto della disciplina sulla protezione dei dati personali, degli ‘interessi commerciali’, dei diritti di proprietà intellettuale e di proprietà industriale. Inoltre, è prescritto che tali dati debbano rispettare i requisiti di reperibilità, accessibilità, interoperabilità e riutilizzabilità.

Quanto, poi, alla possibilità di stipulare accordi di esclusiva, il comma 13 – modificando l'art. 11 del D.Lgs. n. 36/2006 – prevede che essi possano essere conclusi solo ove necessari, ossia se per l'erogazione di un servizio d'interesse pubblico è necessario un diritto esclusivo, e che comunque la fondatezza del motivo di attribuzione dell'esclusiva sia soggetta a valutazione periodica (con cadenza almeno triennale). In ogni caso, tali accordi devono contenere termini trasparenti e pubblicati sul sito istituzionale prima che abbiano effetto. La disciplina dell'art. 11 trova applicazione anche con riferimento alle disposizioni che, pur non concedendo espressamente un'esclusiva, limitano la possibilità di riutilizzo dei documenti da parte di terzi rispetto all'accordo.

Il comma 14 modifica l'art. 12 del decreto del 2006, stabilendo che l'Agenzia per l'Italia digitale (AgID) adotti le linee guida contenenti le regole tecniche per l'attuazione del D.Lgs. n. 200/2021.

Il comma 15, infine, inserisce un nuovo articolo (12-*bis*) al D.Lgs. n. 36/2006, riguardante specifiche serie di dati di elevato valore, individuate dalla Commissione europea ai sensi dell'art. 14, paragrafo 1 della *Open Data Directive*. Tali serie debbono essere rese disponibili gratuitamente, leggibili meccanicamente, fornite mediante API e mediante *download* in blocco, se del caso.

Infine, gli articoli 2 e 3 del D.Lgs. n. 200/2021 prevedono, rispettivamente, l'abrogazione dell'art. 3 del D.Lgs. 18 maggio 2015, n. 102 (che aveva dato attuazione alla direttiva 2013/37/UE, modificativa della menzionata direttiva 2003/98/CE) e l'esclusione di nuovi o maggiori oneri per la finanza pubblica derivanti dall'attuazione del decreto.

RICCARDO ALFONSI

<https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2021-11-08;200>

2022/1(3)EMI

### **L'attuazione della direttiva (UE) 2018/1972 che istituisce il Codice europeo delle comunicazioni elettroniche (D. Lgs. 8 novembre 2021, n. 207, modificativo del D. Lgs. 259/2003)**

Il 24 dicembre 2021 è entrato in vigore il Decreto Legislativo n. 207 dell'8 novembre 2021 (il “**Decreto**”), che dà attuazione alla direttiva (UE) 2018/1972 relativa al Codice europeo delle comunicazioni elettroniche (innanzi anche solo il “**Codice**”).

In precedenza, il 4 febbraio 2021, l'Italia insieme ad altri 24 Stati membri era stata sanzionata per il ritardo nel recepimento della direttiva, il cui termine finale era stato previsto per il 21 dicembre 2020.

Il Decreto va a sostituire i primi 98 articoli del Codice delle comunicazioni elettroniche (D. Lgs. 259/2003) e, di fatto, incide profondamente sulla previgente disciplina.

Esso, infatti, riguarda sia le reti e ed i servizi di comunicazione elettronica ad uso pubblico sia le reti ed i servizi di comunicazione elettronica ad uso privato, oltre a disciplinare il mercato delle reti di comunicazione per la diffusione circolare di programmi sonori e televisivi nonché tutti i servizi radioelettrici e a predisporre strumenti di tutela degli impianti sottomarini di comunicazione elettronica.

Le novità più rilevanti attengono agli obblighi di trasparenza imposti agli operatori, la durata dei contratti ed il diritto di recesso. Sono riconosciuti maggiori poteri all'Autorità per le Garanzie nelle Comunicazioni e si prevedono modifiche in materia edilizia.

In merito agli obblighi di trasparenza per gli operatori, a norma dell'art. 98-*septies decies* del Codice, «se il contratto prevede la proroga automatica di un contratto», essi informano «l'utente finale, in modo chiaro e tempestivo e su un supporto durevole, circa la fine dell'impegno contrattuale e in merito alle modalità di recesso dal contratto e migliori tariffe relative ai loro servizi», e sono tenuti almeno una volta all'anno ad aggiornare gli utenti finali in merito alle migliori tariffe.

Per quanto concerne la durata dei contratti, essa non può essere superiore ai 24 mesi, con l'obbligo in capo ai fornitori di prevedere che tra le offerte commerciali almeno una abbia una durata massima iniziale di 12 mesi.

Il diritto di recesso dell'utente viene rafforzato ulteriormente. Si prevede, difatti, che l'utente finale abbia il diritto di recedere dal contratto in qualsiasi momento con un preavviso di massimo un mese, nel caso in cui sia prevista la proroga automatica del contratto. In ogni modo, l'utente può esercitare il suo diritto di recesso entro sessanta giorni dall'avvenuta comunicazione di modifica delle condizioni contrattuali. Inoltre, i fornitori sono tenuti ad informare «gli utenti finali, con preavviso non inferiore a trenta giorni, di qualsiasi modifica delle condizioni contrattuali e, al contempo, del loro diritto di recedere dal contratto senza incorrere in alcuna penale né ulteriore costo di disattivazione se non accettano le nuove condizioni» (nuovo art. 98-*septies decies* del Codice).

Sono notevolmente ampliati i poteri sanzionatori concessi all'Autorità per le Garanzie nelle Comunicazioni, come si evince dall'art. 30 del Decreto. Nello specifico, l'AGCOM può emettere sanzioni amministrative pecuniarie nei confronti di imprese aventi significativo potere di mercato non inferiori al 2 per cento e non superiore al 5 per cento del fatturato realizzato nell'ultimo bilancio approvato anteriormente alla notificazione della contestazione e relativo al mercato al quale l'inottemperanza si riferisce.

Il Decreto affronta anche alcune questioni disciplinate dal testo Unico per l'edilizia. In particolare, per le nuove costruzioni e per gli interventi su edifici esistenti si richiede l'equipaggiamento digitale e l'attestazione tramite una specifica etichetta di «edificio predisposto alla banda ultra larga».

Inoltre, viene modificato anche l'art. 24 del testo Unico per l'edilizia dedicato all'agibilità degli edifici, sancendo che tra le condizioni della segnalazione certificata di agibilità rientra la certificazione dell'avvenuto rispetto degli obblighi di infrastrutturazione digitale.

In conclusione, si può notare che il nuovo Codice europeo delle comunicazioni elettroniche va ad incidere sia su profili concorrenziali del mercato sia sul fronte della tutela del consumatore, assumendo una prospettiva ampia di disciplina.

ENZO MARIA INCUTTI

<https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2021;207>

2022/1(4)SO

**Verso il Data Act: la proposta di Regolamento del Parlamento e del Consiglio su regole armonizzate sull'accesso equo e l'uso dei dati (legge sui dati) COM(2022) 68 final del 23.2.2022**

Con il documento COM(2022) 68 *final* del 23 febbraio 2022, recante “Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'accesso equo e l'uso dei dati (legge sui dati)” (la “**Proposta di Data Act**”), la

Commissione europea ha pubblicato una proposta di regolamento che si aggiunge agli ormai numerosi interventi riferiti sin nella loro intitolazione ai “dati”. Oltre al GDPR del 2016 “Regolamento generale sulla protezione dei dati” (Reg. UE 2016/679) possiamo citare il “Regolamento sulla libera circolazione dei dati non personali” del 2018 (Reg. UE 2018/1807), la direttiva “Open Data” del 2019 (Direttiva UE 2019/1024 relativa alla “apertura dei dati e al riutilizzo dell’informazione del settore pubblico” attuata da parte del legislatore italiano con D. Lgs. 8 novembre 2021 n. 200, su cui v. la notizia [2021/1\(2\)GP](#) *supra*) e la Proposta di “Data Governance Act” del 2020, (Proposta di “regolamento relativo alla *governance* europea dei dati”, del 25 novembre 2020) su cui v. la notizia [2021/4\(4\)RA](#).

La Proposta di *Data Act* comprende una bozza di regolamento (la “**Bozza di Regolamento**”) ed una relazione esplicativa (la “**Relazione**”).

Il **Capo I** della Bozza di Regolamento (artt. 1-2) ne definisce l’oggetto e il campo di applicazione e contiene le definizioni utilizzate nel corpo del provvedimento. In particolare, secondo l’art. 1 par. 1, il regolamento “stabilisce regole armonizzate sulla messa a disposizione all’utente di un prodotto o di un servizio correlato, di dati generati dall’uso

di tale prodotto o servizio, sulla messa a disposizione di dati da parte dei *data holders* ai *data recipients*, e sulla messa a disposizione di dati da parte dei *data holders* a organi del settore pubblico o istituzioni dell’Unione, agenzie o organi, laddove si verifichi una necessità eccezionale, per l’esecuzione di un compito svolto nel pubblico interesse”. L’art. 2 offre la stessa definizione di ‘dati’ contenuta nella Proposta di *Data Governance Act* del 2020, ossia “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”. Le definizioni di prodotto e di servizio correlato sono, rispettivamente, le seguenti: “‘prodotto’ significa un oggetto tangibile e mobile, anche se incorporato in un oggetto immobile, che ottiene, genera o raccoglie dati concernenti il suo uso o ambiente e che è capace di comunicare dati attraverso un servizio pubblicamente disponibile di comunicazione elettronica e la cui funzione primaria non consista nell’immagazzinamento e trattamento di dati”, “‘servizio correlato’ significa un servizio digitale, compreso il *software*, che è incorporato o inter-connesso con un prodotto in modo tale che la sua assenza impedirebbe al prodotto di eseguire una delle sue funzioni”. L’ ‘utente’ è definito come “una persona fisica o giuridica che possiede, affitta o noleggia un prodotto o riceve un servizio”. Il ‘*data holder*’ è definito come “una persona giuridica o fisica che ha il diritto o l’obbligo, ai sensi di questo Regolamento, del diritto dell’Unione applicabile o del diritto nazionale che dà attuazione al diritto dell’Unione, o, in caso di dati non personali e attraverso il controllo del disegno tecnico del prodotto e dei servizi correlati, la capacità, di mettere a disposizione certi dati”. Il ‘*data recipient*’ è definito come “una persona giuridica o fisica, che agisce per fini connessi alla sua attività professionale, commerciale o artigianale, diversa dall’utente di un prodotto o di un servizio correlato, al quale il *data holder* mette a disposizione dati, inclusi terzi in conseguenza di una richiesta dell’utente al *data holder* o in conformità a un obbligo discendente dal diritto dell’Unione o dal diritto nazionale che dà attuazione al diritto dell’Unione”. Tra le altre, l’art. 2 contiene anche una definizione di ‘smart contract’ quale “programma per elaboratore conservato in un sistema di registro elettronico laddove il risultato dell’esecuzione del programma è registrato nel registro elettronico” e rinvia per la definizione di ‘registro elettronico’ ad una definizione a sua volta oggetto della recente proposta della Commissione (COM(2021) 281 recante la “Proposta di un regolamento che modifichi il Regolamento (UE) n. 910/2014 per quanto riguarda l’istituzione di un quadro per un’identità digitale europea”).

Il **Capo II** (artt. 3-7) è - secondo la Relazione - inteso ad aumentare la certezza per i consumatori e le imprese di accedere ai dati generati dai prodotti e dai servizi correlati che

essi utilizzano. Secondo la sintesi contenutistica e finalistica indicata nella Relazione, le norme di questo Capo prevedono che i prodotti e i servizi debbano essere progettati in un modo che renda i dati facilmente accessibili “*by default*” e che gli utenti debbano essere informati su quali dati sono accessibili e sulle modalità di accesso. L’art. 4 prevede che i dati debbano essere messi a disposizione dell’utente senza costi e, ove non direttamente accessibili, dietro semplice richiesta dell’utente. Sono previste alcune disposizioni che condizionano il diritto di accesso in relazione a segreti commerciali, come definiti dalla Direttiva (UE) 2016/943, e altre che vietano all’utente di utilizzare i dati ottenuti dal *data holder* per sviluppare prodotti che competono con il prodotto da cui generano i dati. Laddove si tratti di dati personali e l’utente non sia la persona interessata, il *data holder* può rendere tali dati personali accessibili all’utente soltanto nel rispetto delle condizioni previste dall’art. 6, par. 1 del GDPR, e, ove applicabile, dall’art. 9 del GDPR. Infine, l’art. 4 prevede che il *data holder* può utilizzare i dati non personali soltanto sulla base di un accordo con l’utente, e vieta al *data holder* di utilizzare i dati per trarne delle informazioni di natura economica, patrimoniale o industriale sull’utente che possano danneggiare la posizione commerciale dell’utente nei mercati in cui l’utente è attivo. L’art. 5 prevede il diritto dell’utente di chiedere al *data holder* di mettere i dati a disposizione di terzi senza spese per l’utente. L’art. 5 prevede che non possano agire per ottenere i dati ai sensi dell’art. 4 le imprese che forniscono servizi di piattaforma di base che hanno requisiti per qualificarsi come *gatekeepers* ai sensi del (non ancora approvato) *Digital Markets Act*, sul quale v. la notizia [2021/1\(4\)EMI](#). L’art. 6 prevede gli obblighi e i divieti in capo ai terzi ai quali vengono messi a disposizione i dati ai sensi dell’art. 5. È previsto che il trattamento dei dati da parte di questi soggetti debba essere limitato alle finalità e alle condizioni concordate con l’utente, nel rispetto dei diritti della persona interessata, relativamente ai dati personali, e con obbligo di cancellazione dei dati quando essi cessano di essere necessari per la finalità concordata. Tra i divieti è previsto anche in capo ai terzi il divieto di mettere i dati a disposizione di imprese che forniscono servizi di piattaforma di base che hanno i requisiti per qualificarsi come *gatekeepers* ai sensi del (non ancora approvato) *Digital Markets Act*. Infine, l’art. 7 dispone che gli obblighi di questo Capo non si applicano ai dati generati da prodotti realizzati o da servizi correlati prestati da piccole e microimprese (ai sensi dell’Articolo 2 dell’Allegato alla Raccomandazione 2003/361/CE).

Il **Capo III** (artt. 8-12) detta alcune regole da osservarsi allorché i *data holders* sono obbligati (o sulla base di quanto previsto nel Capo II o sulla base di altre disposizioni del diritto dell’Unione o degli Stati membri) a mettere i dati a disposizione dei *data recipients*. Secondo la sintesi di cui alla Relazione, le disposizioni degli articoli 8 e 9 prevedono che le condizioni della messa a disposizione dei dati da parte dei *data holders* in favore dei *data recipients* debbano essere “*fair*” e non discriminatorie, e che, laddove sia previsto un corrispettivo, esso debba essere “*reasonable*”, senza pregiudizio per altre disposizioni del diritto dell’Unione o del diritto nazionale derivato di escludere o ridurre un simile corrispettivo. È previsto in ogni caso che ai *data recipients* aventi le dimensioni di microimprese, piccole o medie imprese (come definite ai sensi dell’Articolo 2 dell’Allegato alla Raccomandazione 2003/361/CE) non possa essere chiesto un corrispettivo il cui importo ecceda i costi sopportati dai *data holders* per mettere i dati a loro disposizione, salvo che sia diversamente previsto nelle legislazioni di settore. L’art. 10 prevede che organi speciali, certificati dagli Stati membri, siano dedicati alla risoluzione di controversie tra *data holders* e *data recipients* aventi ad oggetto la determinazione delle condizioni di messa a disposizione dei dati ai sensi degli articoli 8 and 9.

Il **Capo IV** (composto del solo art. 13) intitolato “*Unfair terms related to data access and use between enterprises?*” riguarda le clausole contrattuali concernenti l’accesso a dati o l’uso di dati o la responsabilità e i rimedi per l’inadempimento o l’estinzione di obbligazioni relative a dati,

che siano “imposte unilateralmente” da imprese a microimprese, piccole o medie imprese (come definite ai sensi dell’Articolo 2 dell’Allegato alla Raccomandazione 2003/361/CE). L’art. 13 ricalca la terminologia e la tecnica normativa della direttiva 93/13/CEE sulle clausole abusive nei contratti stipulati con i consumatori. Secondo la sintesi della Relazione, l’obiettivo è quello di impedire che gli accordi contrattuali sull’accesso ai dati e l’uso di dati consentano di profittare di squilibri nel potere negoziale tra le parti contraenti. Lo strumento del test di “*unfairness*” prevede una definizione generale di abusività e due elenchi di clausole, uno relativo a clausole da intendersi in ogni caso abusive (tra cui quelle che consentono al predisponente di determinare la “conformità dei dati al contratto”) e l’altro di clausole che si presumono abusive. L’art. 34 (contenuto nel Capo IX) prevede che la Commissione debba predisporre e raccomandare modelli non vincolanti di contratto sull’accesso ai dati e l’uso di dati come strumento di ausilio alle parti nella redazione e negoziazione di contratti con diritti e doveri contrattuali equilibrati.

Il **Capo V** (artt. 14-22) è inteso a creare, secondo la presentazione della Relazione, un quadro armonizzato di regole per l’uso da parte di organi del settore pubblico e istituzioni dell’Unione di dati detenuti da imprese in situazioni nelle quali si riscontra una esigenza eccezionale dei dati richiesti. Il quadro si basa su un obbligo di mettere i dati a disposizione che sorge solo in caso di emergenze pubbliche ovvero in situazioni in cui gli organi del settore pubblico hanno una esigenza eccezionale di utilizzare certi dati, ma tali dati non possono ottenersi sul mercato, o in modo tempestivo attraverso l’emanazione di una nuova legislazione o per mezzo di obblighi già esistenti. È previsto che nel caso di un’esigenza eccezionale di rispondere ad una emergenza pubblica, come emergenze di salute pubblica o grandi disastri naturali o indotti dall’uomo, i dati dovranno essere messi a disposizione gratuitamente. In altri casi di esigenza eccezionale, incluso il caso di esigenze legate alle conseguenze di una emergenza pubblica, il *data holder* che mette i dati a disposizione ha diritto a una remunerazione comprensiva dei costi più un margine ragionevole. Per evitare abusi, è previsto che le richieste debbano essere proporzionate, che esse debbano indicare chiaramente gli obiettivi che si intendono perseguire e che rispettino gli interessi dei *data holder* che mettono i dati a disposizione. È previsto che autorità competenti *ad hoc* siano investiti del compito di assicurare la trasparenza e la pubblicazione di tutte le richieste e di gestire le relative eventuali doglianze.

Il **Capo VI** (artt. 23-26) prevede in capo ai fornitori di servizi *cloud*, *edge* ed altri servizi di trattamento di dati una serie di requisiti di natura contrattuale, commerciale e tecnica al fine di consentire la commutazione tra tali servizi. In particolare, la Proposta di *Data Act*, secondo la Relazione, mira ad assicurare che i clienti mantengano un minimo livello di funzionalità del servizio dopo che essi hanno ottenuto la commutazione in favore di un altro fornitore del servizio. La Proposta di *Data Act* contiene una eccezione per il caso di impraticabilità tecnica della commutazione, ma pone l’onere della prova al riguardo in capo al fornitore del servizio. La Proposta di *Data Act* non prevede standard tecnici delle interfacce, ma richiede che i servizi siano compatibili con gli standards europei, o, ove disponibili, con le specificazioni tecniche di interoperabilità aperta.

Il **Capo VII** (composto del solo art. 27) mira a contrastare l’accesso illegittimo ai dati non personali detenuti nell’Unione da fornitori di servizi di trattamento dei dati offerti nel mercato dell’Unione. Al riguardo sono previsti in capo ai fornitori di servizi di trattamento dei dati una serie di obblighi di salvaguardia di natura tecnica, legale e organizzativa.

Il **Capo VIII** (artt. 28-30) prevede alcune prescrizioni relative all’interoperabilità per gli operatori di “*data spaces*” e per i fornitori di servizi di trattamento di dati nonché alcuni requisiti per gli *smart contracts*.

Il **Capo IX** (art. 31 -34) prevede *inter alia* che gli Stati membri designino una o più autorità competenti per l'applicazione delle disposizioni del Regolamento, per l'esame di doglianze nonché per l'irrogazione di sanzioni per il caso di violazioni delle medesime disposizioni.

Il **Capo X** (composto del solo art. 35) prevede che il diritto *sui generis* di cui alla direttiva sulle banche di dati (Direttiva 96/9/CE) non si applichi alle banche di dati ottenute o generate dall'uso di un prodotto o di un servizio correlato. La Relazione spiega che tale previsione mira ad evitare che possano essere compromessi i diritti degli utenti ai sensi degli articoli 4 e 5 del Regolamento.

Infine, il **Capo XI** permette alla Commissione di adottare atti delegati per introdurre un meccanismo di monitoraggio sulle tariffe di commutazione imposte ai fornitori di servizi di trattamento di dati, al fine di specificare i requisiti essenziali riguardanti l'interoperabilità, e di pubblicare informazioni relative alle specificazioni e agli standard di interoperabilità. Si prevede inoltre l'adozione di specifiche tecniche comuni per gli *smart contracts* per l'ipotesi di carenza o insufficienza di *standards* armonizzati idonei a garantire la conformità ai requisiti essenziali previsti dal Regolamento.

SALVATORE ORLANDO

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068&from=EN>

2022/1(5)ST

### **La proposta di Dichiarazione europea sui diritti e i principi digitali per il decennio digitale COM(2022) 28 final del 26 gennaio 2022.**

Il 26 gennaio 2022 la Commissione ha proposto una dichiarazione solenne interistituzionale sui diritti e i principi digitali per il decennio digitale: la *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, del Parlamento europeo, del Consiglio e della Commissione (di seguito anche la “**Dichiarazione**”). Alla base della proposta, c'è la consapevolezza che l'accelerazione della trasformazione digitale e il suo pervadere ogni aspetto della vita delle persone rende sempre più importante che l'Unione Europea specifichi come applicare i suoi valori e i diritti fondamentali nel mondo *online*, non solo con provvedimenti puntuali e relativi a singoli settori, ma anche in modo trasversale e generale.

Il modello di trasformazione digitale auspicato mira a “rafforzare la dimensione umana dell'ecosistema digitale”, nel pieno rispetto dei diritti fondamentali, del diritto alla protezione dei dati e alla non discriminazione, nonché dei principi di inclusività e di neutralità tecnologica e della rete. Il modello proposto è imperniato sul mercato unico digitale e basato su una tecnologia che contribuisca alla lotta ai cambiamenti climatici e alla protezione dell'ambiente. Sul punto la proposta *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale* si pone in continuità con la [Dichiarazione di Tallinn sull'e-government](#), firmata il 6 Ottobre 2017 da tutti gli Stati membri dell'UE e dai paesi dell' *European Free Trade Association (EFTA)* (<https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration>), con la [Dichiarazione di Berlino sulla società digitale e su un governo digitale fondato sui valori](#), firmata l'8 Dicembre 2020 dai ministri responsabili di tutti gli Stati membri dell'UE (<https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government>) e con la [Dichiarazione di Lisbona - "Democrazia digitale con uno scopo"](#), presentata all'Assemblea sul digitale nel Giugno 2021

<https://futurium.ec.europa.eu/en/digital-compass/digital-principles/library-video/lisbon-declaration-digital-democracy-purpose?language=it-video/lisbon-declaration-digital-democracy-purpose?language=it>.

La Dichiarazione si articola in sei capitoli, che hanno i seguenti contenuti.

**Capitolo I: mettere le persone al centro della trasformazione digitale.** Al fine di mettere concretamente le persone al centro della trasformazione digitale occorre impegnarsi a:

- rafforzare il quadro democratico per una trasformazione digitale che vada a beneficio di ogni persona e migliori la vita di tutti gli europei;
- adottare le misure necessarie per garantire che i valori dell'Unione e i diritti delle persone riconosciuti dal diritto dell'Unione siano rispettati *online* così come *offline*;
- promuovere un'azione responsabile e diligente da parte di tutti gli attori digitali, pubblici e privati, per un ambiente digitale sicuro e protetto;
- promuovere attivamente questa visione della trasformazione digitale, anche nelle relazioni internazionali.

**Capitolo II: solidarietà e inclusione.** Il dovere di rispettare la persona umana e la sua dignità prescindono dal luogo o dal tempo nel quale ciascuno esplica la sua personalità.

La dimensione *online* delle nostre vite non può certamente prescindere dalla solidarietà e dall'inclusione. Anche le soluzioni tecnologiche devono, pertanto, consentire l'esercizio dei diritti, promuovere l'inclusione e “perseguire una trasformazione digitale che non lasci indietro nessuno, che includa in particolare gli anziani, le persone con disabilità, le persone emarginate, vulnerabili o prive di diritti, così come coloro che agiscono per loro conto”.

A tal fine è necessario che tutti gli operatori del mercato che traggono vantaggio dalla trasformazione digitale si assumano le proprie responsabilità sociali e contribuiscano in modo equo e proporzionato ai costi delle infrastrutture, dei servizi e dei beni pubblici, a beneficio di tutti gli europei.

La solidarietà e l'inclusione nel mondo digitale non possono prescindere dalla **connettività** digitale ad alta velocità a prezzi accessibili, indipendentemente dal luogo in cui le persone vivono e dal loro reddito, garantendo un'internet neutra e aperta in cui le applicazioni, i servizi e i contenuti non siano bloccati o degradati in modo ingiustificato. L'**inclusione** non può che realizzarsi attraverso il diritto all'istruzione, alla formazione e all'apprendimento al fine di acquisire **competenze digitali** di base e comunque necessarie per partecipare attivamente all'economia, alla società e ai processi democratici.

Le competenze digitali sono uno dei quattro punti cardine della proposta di decisione presentata dalla Commissione “*Path to the Digital Decade*” del 15 Settembre 2021 ([https://ec.europa.eu/commission/presscorner/detail/it/ip\\_21\\_4630](https://ec.europa.eu/commission/presscorner/detail/it/ip_21_4630)). Neppure si può prescindere da **condizioni di lavoro** eque, giuste, sane e sicure e, a tal fine, occorre proteggere il lavoratore nell'ambiente digitale, così come nel luogo di lavoro fisico, garantendo che tutti abbiano la possibilità di disconnettersi e di godere di garanzie per l'equilibrio tra vita professionale e vita privata. Ogni persona dovrebbe avere **accesso a tutti i servizi pubblici principali online** in tutta l'Unione. A nessuno deve essere chiesto di fornire dati più spesso di quanto necessario durante l'accesso ai servizi pubblici digitali e il loro utilizzo. Strategica diventa a tal fine la garanzia di un'identità digitale accessibile, sicura, affidabile e che consenta l'accesso ai servizi *online*, alle informazioni della Pubblica amministrazione ed ai servizi sanitari e assistenziali digitali concepiti per soddisfare le esigenze dei cittadini, comprese le cartelle cliniche.

**Capitolo III: libertà di scelta.** Nella Dichiarazione emerge la consapevolezza che gli algoritmi influenzano così tanto la nostra vita, dagli aspetti più insignificanti a quelli più importanti, che è persino la libertà di scelta a risentirne, a volte anche inconsapevolmente. Il

Capitolo III della Dichiarazione infatti, dedicato alla libertà di scelta, si apre con il riferimento a **Interazioni con algoritmi e sistemi di intelligenza artificiale**.

Ogni persona, si legge, “dovrebbe essere messa nelle condizioni di godere dei benefici offerti dall'intelligenza artificiale facendo le proprie scelte informate nell'ambiente digitale, e rimanendo al contempo protetta dai rischi e dai danni alla salute, alla sicurezza e ai diritti fondamentali”.

A tal fine occorre garantire:

- la trasparenza in merito all'uso degli algoritmi e dell'intelligenza artificiale e fare in modo che le persone, quando interagiscono con essi, siano autonome, responsabili e informate;
- che i sistemi algoritmici siano basati su insiemi di dati adeguati, al fine di evitare discriminazioni illecite, e consentano la supervisione umana dei risultati che riguardano le persone;
- che le tecnologie come gli algoritmi e l'intelligenza artificiale non siano utilizzate per predeterminare le scelte delle persone, ad esempio per quanto riguarda la salute, l'istruzione, l'occupazione e la vita privata;
- che i sistemi digitali e di intelligenza artificiale siano sicuri e vengano utilizzati nel pieno rispetto dei diritti fondamentali delle persone.

A tal fine devono essere ben definite le responsabilità delle piattaforme, in particolare dei grandi operatori e dei *gatekeeper*, e deve garantirsi che ogni persona possa scegliere realmente quali servizi *online* utilizzare, sulla base di informazioni obiettive, trasparenti e affidabili.

**Capitolo IV: partecipazione allo spazio pubblico digitale.** Quanto detto per l'inclusione e la solidarietà vale anche per la libertà di espressione che non può certo essere mortificata per il fatto che si espliciti *online*. Ogni persona dovrebbe avere accesso a un ambiente *online* affidabile, sicuro, diversificato e multilingue. L'accesso a contenuti diversificati contribuisce a un dibattito pubblico pluralistico e dovrebbe consentire a tutti di partecipare al processo democratico. Ogni persona dovrebbe disporre dei mezzi per sapere chi possiede o controlla i servizi mediatici che utilizza. Il ruolo delle piattaforme online, specialmente se di grandi dimensioni, è ormai innegabile, godendo le stesse di un'autorità di fatto e di uno statuto privatistico che mal si concilia con la loro attività potenzialmente capace di produrre effetti rilevanti anche sul piano pubblicitario e istituzionali. Le piattaforme online di dimensioni molto grandi dovrebbero sostenere il libero dibattito democratico online, visto il ruolo svolto dai loro servizi nel plasmare l'opinione pubblica e il dibattito pubblico. Dovrebbero attenuare i rischi derivanti dal funzionamento e dall'uso dei loro servizi, anche in relazione alle campagne di disinformazione, e tutelare la libertà di espressione.

A tal fine occorre adottare misure volte a contrastare tutte le forme di contenuti illegali proporzionalmente al danno che possono causare e nel pieno rispetto del diritto alla libertà di espressione e di informazione, senza imporre obblighi generali di sorveglianza. Si evocano sul punto le scelte fatte con la Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, COM(2020) 825 *final* del 15 dicembre 2020, nota come *Digital Services Act*. (su cui v. la notizia [2021/1\(3\)ST](#)).

**Capitolo V: sicurezza, protezione e conferimento di maggiore autonomia e responsabilità.** Un ambiente online sicuro e protetto è un ambiente nel quale tecnologie, prodotti e servizi digitali, già nella fase di progettazione, sono tali da tutelare la **vita privata delle persone**, la loro **identità digitale** e il diritto alla protezione dei propri dati personali *online*. Tale diritto comprende il **controllo individuale sui dati**, su come sono utilizzati e sui soggetti con i quali sono condivisi. Ogni persona ha diritto alla riservatezza delle proprie comunicazioni e delle informazioni sui propri dispositivi elettronici e nessuno può essere sottoposto a misure illecite di sorveglianza o intercettazione *online*.

Ogni persona dovrebbe essere in grado di determinare la propria eredità digitale e decidere cosa succede, dopo la sua morte, alle informazioni pubblicamente disponibili che la riguardano.

Particolarmente delicato è il problema della garanzia di una partecipazione *online* adeguata all'età; problema che la Dichiarazione non trascura, allorché prevede che **i bambini e i giovani *online* dovrebbero essere protetti e dotati di maggiore autonomia e responsabilità**. Anche a tal fine non si può prescindere da offrire adeguate opportunità per consentire ai giovani, anche minori, capacità e competenze necessarie per navigare nell'ambiente *online* in modo attivo e sicuro, per compiere scelte informate *online* e esprimere, anche in tale ambito, la propria creatività.

Soprattutto con riferimento a questi soggetti, potenzialmente più vulnerabili degli adulti, non si può prescindere da strumenti idonei a proteggerli dai contenuti dannosi e illegali, dallo sfruttamento, dalla manipolazione e dagli abusi *online*, impedendo che lo spazio digitale sia utilizzato per commettere o facilitare reati.

I minori hanno il diritto di essere protetti da tutti i reati commessi o facilitati attraverso le tecnologie digitali.

**Capitolo VI: sostenibilità.** Favorire lo sviluppo e l'utilizzo di tecnologie digitali sostenibili significa favorire lo sviluppo e l'utilizzo di tecnologie che abbiano un impatto ambientale minimo e sviluppare e diffondere soluzioni digitali con ricadute positive per l'ambiente e il clima.

A tal fine è necessario promuovere un'economia circolare nella quale prodotti e servizi digitali siano progettati, prodotti, utilizzati, smaltiti e riciclati in modo da ridurre al minimo il loro impatto negativo a livello ambientale e sociale.

Soprattutto è necessario consentire ad ogni persona di dare un contributo concreto alla sostenibilità e attraverso le proprie scelte. Ma ciò è possibile solo se è consentito a ciascuno di avere accesso a informazioni precise e di facile comprensione sull'impatto ambientale e sul consumo energetico dei prodotti e dei servizi digitali, in modo da essere in grado di compiere scelte responsabili.

SARA TOMMASI

<https://digital-strategy.ec.europa.eu/en/news/commission-puts-forward-declaration-digital-rights-and-principles-everyone-eu>

2022/1(6)SO

## **La proposta di Regolamento del Parlamento e del Consiglio relativo alla trasparenza e al targeting della pubblicità politica COM(2021) 731 final del 25 novembre 2021**

Con il documento COM(2021) 731 *final* del 25 novembre 2021, recante “Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla trasparenza e al targeting della pubblicità politica”, la Commissione europea ha pubblicato una proposta di regolamento in materia di “pubblicità politica” che comprende una bozza di regolamento (la “**Bozza di Regolamento**”) ed una relazione esplicativa (la “**Relazione**”).

Nella Relazione, è specificato che scopo della proposta è contribuire al buon funzionamento del mercato interno della pubblicità politica con norme armonizzate – indirizzate ai prestatori di servizi di pubblicità politica - che garantiscano un livello di trasparenza elevato della pubblicità politica e servizi connessi. Altro scopo della proposta,

indicato nella Relazione, è quello di tutelare le persone fisiche con riguardo al trattamento dei dati personali, in particolare attraverso norme sull'uso delle tecniche di *targeting* e della c.d. “amplificazione” sempre in ambito di pubblicità politica. La Bozza di Regolamento prevede che tali norme si applicheranno a tutti i titolari del trattamento - quindi non solo ai prestatori di servizi di pubblicità politica - che fanno uso delle tecniche di *targeting* e “amplificazione”. L’art. 2 della Bozza di Regolamento definisce le ‘tecniche di targeting o amplificazione’ come segue: “*le tecniche usate per rivolgere solo a una persona specifica o a un gruppo specifico di persone un messaggio di pubblicità politica concepito su misura, o per aumentarne la diffusione, la portata o la visibilità*”.

Nella Relazione si osserva che i servizi di pubblicità politica sono in fase di espansione nell’UE, e che, a fronte di ciò, il quadro, già molto frammentato, delle norme nazionali, è reso ancor maggiormente frammentario dalle innovazioni tecnologiche della comunicazione e dalla necessità degli Stati membri, di dare risposte alle nuove, conseguenti, forme della pubblicità politica. La Relazione riconosce che i dati personali dei cittadini dell’Unione sono utilizzati per indirizzare messaggi politici e per amplificarne l’impatto e la diffusione, con precisi rischi di ripercussioni negative sui diritti fondamentali dei cittadini, tra cui la libertà di opinione e informazione, nel prendere decisioni politiche ed esercitare il diritto di voto.

Nella Relazione si affronta il tema della coerenza della proposta con le disposizioni vigenti nel settore interessato e con le altre normative dell’Unione, così come si dà conto della base giuridica utilizzata, della sussidiarietà (per competenza non esclusiva), della proporzionalità e si motiva quindi in merito allo strumento del regolamento. Nell’ambito dell’esposizione sulla valutazione di impatto, la Relazione dichiara che le misure proposte hanno tutte un impatto positivo sui diritti fondamentali, ovvero che eventuali impatti negativi non dovrebbero essere significativi. In particolare, a questo riguardo, la Relazione osserva e dichiara che la proposta impone restrizioni limitate alla libertà di espressione e di informazione (art. 11 della Carta dei diritti fondamentali dell’Unione europea “CDFUE”), al diritto alla vita privata (art. 7 CDFUE) e al diritto alla protezione dei dati di carattere personale (art. 8 CDFUE), ma soggiunge che tali restrizioni sono proporzionate e limitate al minimo necessario.

Il **Capo I** della Bozza di Regolamento (artt. 1-3) ne definisce l’oggetto e il campo di applicazione, contiene le definizioni dei termini principali e il livello di armonizzazione delle misure.

Il **Capo II** (artt. 4-11) tratta degli obblighi di trasparenza applicabili alla pubblicità politica a pagamento; stabilisce le misure applicabili a tutti i prestatori di servizi di pubblicità politica che concorrono alla preparazione, collocazione, promozione, pubblicazione o diffusione di pubblicità politica; in particolare dispone in ordine alla trasparenza della pubblicità politica (art. 4), all’obbligo di identificare i messaggi di pubblicità politica (art. 5) e all’obbligo di registrare e trasmettere informazioni agli editori di pubblicità politica (art. 6). In questo capo si prevedono anche ulteriori obblighi applicabili ai soli editori di pubblicità politica, in aggiunta a quelli di cui agli articoli 4, 5 e 6. In particolare, gli editori devono includere in ciascun messaggio di pubblicità politica una dichiarazione attestante chiaramente che si tratta di pubblicità politica, indicare il nome dello sponsor e pubblicare informazioni che rendano comprensibili il contesto più ampio in cui si situa il messaggio e i suoi obiettivi (art. 7). Gli editori di pubblicità politica devono inoltre pubblicare annualmente informazioni sugli importi fatturati e sul valore di altre prestazioni percepite in cambio parziale o integrale dei servizi prestati in relazione a messaggi di pubblicità politica (art. 8), e devono infine mettere in atto meccanismi di facile uso perché i cittadini possano segnalare i messaggi di pubblicità politica che non rispettano gli obblighi stabiliti dal regolamento (art. 9).

Gli artt. 10 e 11 prevedono che i prestatori di servizi di pubblicità politica devono trasmettere le informazioni pertinenti alle autorità competenti e ad altri soggetti interessati come previsti nell’art. 11.

Il **Capo III** (artt. 12-13), intitolato “*Targeting e amplificazione della pubblicità politica*” disciplina l'uso delle ‘tecniche di *targeting* o amplificazione’ che comportano il trattamento di dati personali a fini di pubblicità politica. È previsto che quando il trattamento riguarda dati sensibili, scatta un divieto cui è possibile derogare solo a precise condizioni. È inoltre prescritto ai responsabili del trattamento che ricorrono a queste tecniche a fini di pubblicità politica di adottare e applicare un “documento di strategia interna che in particolare descriva chiaramente e con linguaggio semplice l'uso di tecniche finalizzate a prendere di mira certi destinatari o amplificare l'impatto”, tenere registri e trasmettere informazioni che permettano agli interessati di comprendere la logica utilizzata e i principali parametri della tecnica applicata e se siano stati usati dati di terzi e altre tecniche analitiche (art. 12). L'articolo 12 stabilisce inoltre ulteriori obblighi a carico degli editori di pubblicità politica. Infine, l'art. 13 prevede che i responsabili del trattamento debbano trasmettere le informazioni ai soggetti interessati ex art. 11.

Il **Capo IV** (artt. 14-17) prevede disposizioni concernenti il controllo e l'esecuzione del regolamento. Si impone ai prestatori di servizi di pubblicità politica non stabiliti nell'Unione l'obbligo di nominare un rappresentante legale in uno degli Stati membri in cui prestano i loro servizi (art. 14). Si stabilisce quali autorità debbano essere incaricate del controllo ed esecuzione delle misure specifiche stabilite dal regolamento. Si fa obbligo agli Stati membri di garantire la cooperazione tra le pertinenti autorità competenti. Si chiede che siano designati punti di contatto ai fini del regolamento e incarica gli Stati membri di garantire lo scambio di informazioni tra gli stessi (art. 15). Si prevede che gli Stati membri debbano stabilire norme sulle sanzioni applicabili in caso di inosservanza degli obblighi dettati dal regolamento (art. 16). Si stabilisce infine l'obbligo in capo agli Stati membri di “pubblicare in luogo visibile le date dei rispettivi periodi elettorali nazionali” (art. 17).

Il **Capo V** (artt. 18-20) contiene le disposizioni finali.

SALVATORE ORLANDO

[https://eur-lex.europa.eu/resource.html?uri=cellar:9cec62db-4dcb-11ec-91ac-01aa75ed71a1.0013.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:9cec62db-4dcb-11ec-91ac-01aa75ed71a1.0013.02/DOC_1&format=PDF)

2022/1(7)ES

**Il Decreto del Ministero dell'economia e delle finanze del 13 gennaio 2022 sull'iscrizione alla sezione speciale del registro dei cambiavalute da parte dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale.**

Il 17 febbraio 2022 è stato pubblicato sulla Gazzetta Ufficiale il Decreto del Ministero dell'economia e delle finanze del 13 gennaio 2022 (il “**Decreto**”). Esso disciplina l'iscrizione alla sezione speciale del registro dei cambiavalute (il “**Registro**”) tenuto dall'Organismo Agenti e Mediatori (l’“**OAM**”) dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale (i “**Prestatori di servizi**”).

Il Decreto attua l'art. 17-*bis*, comma 8-*ter* D. Lgs. 141/2010 che, insieme al comma 8-*bis* del medesimo articolo, sostanzialmente estende la disciplina dei cambiavalute ai Prestatori di servizi ed è stato introdotto dal D. Lgs. 90/2017 attuativo della direttiva 2015/849/UE (c.d. IV direttiva antiriciclaggio) e modificativo del D. Lgs. 231/2007 e del D. Lgs. 109/2007, e a sua volta modificato dal D. Lgs. 125/2019 attuativo della direttiva 2018/843/UE (c.d. V direttiva antiriciclaggio).

Per quanto qui interessa, l'art. 17-*bis*, commi 8-*bis* e *ter* D. Lgs. 141/2010 impone ai Prestatori di servizi di comunicare la loro operatività in Italia, nonché di iscriversi al Registro. Il suddetto comma 8-*ter*, in particolare, delegava ad un decreto del Ministero dell'economia e delle finanze, quello in commento appunto, di stabilire: 1) i tempi e i modi con cui i Prestatori di servizi devono comunicare la propria operatività sul territorio nazionale al suddetto Ministero; 2) le forme di cooperazione tra tale ultimo ente e le forze di polizia per impedire l'esercizio abusivo delle attività relative all'utilizzo di valuta virtuale e di portafoglio digitale.

L'art. 1 del Decreto, similmente al D. Lgs. 231/07, definisce:

(i) il prestatore di servizi relativi all'utilizzo di valuta virtuale come il soggetto “*che fornisce a terzi, a titolo professionale, anche on-line, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore ... nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute*”;

(ii) il prestatore di servizi di portafoglio digitale come colui “*che fornisce, a terzi, a titolo professionale, anche on-line, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti al fine di detenere ... e trasferire valute virtuali*”;

(iii) la valuta virtuale come “*la rappresentazione digitale di valore, non emessa né garantita da una banca centrale ... non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente*”.

Ebbene, da quanto detto emerge che solo i soggetti i quali svolgano “professionalmente” una delle menzionate attività devono ottemperare al provvedimento in parola.

L'art. 3, comma 1 del Decreto stabilisce che i Prestatori di servizi per poter svolgere la propria attività in Italia debbano iscriversi nel Registro. Per farlo, innanzitutto, devono possedere i requisiti di cui all'art. 17-*bis*, comma 2 D. Lgs. 141/2010, ossia la cittadinanza di uno Stato dell'Unione europea, se si tratta di persone fisiche, oppure la sede legale e amministrativa o stabile organizzazione in Italia, se si tratta di persone giuridiche. In secondo luogo, devono inviare una comunicazione all'OAM sulla loro operatività in Italia, verosimilmente prima dell'inizio dell'attività anche se il Decreto non lo specifica. Tale adempimento, ai sensi del combinato disposto degli artt. 17 bis, comma 8 ter D. Lgs. 141/2010 e 3, comma 2 del Decreto, è una condizione essenziale affinché i Prestatori di servizi possano esercitare legittimamente la loro attività.

Coloro i quali siano già operativi alla data di avvio della sezione speciale del registro dei cambiavalute possono inviare la predetta comunicazione entro 60 giorni da tale data. Altrimenti, la loro attività si considera svolta abusivamente (art. 3, comma 3).

La comunicazione, sostanzialmente, deve indicare: i dati del Prestatore di servizi, la tipologia di attività o di servizio forniti e le modalità di svolgimento (art. 3, comma 4). L'OAM verifica la regolarità e completezza della comunicazione ed entro 15 giorni dal ricevimento “*dispone ovvero nega l'iscrizione*” nella sezione speciale del registro dei cambiavalute (art. 3, comma 6). Tale termine può essere sospeso una sola volta per massimo 10 giorni “*qualora l'OAM ritenga la comunicazione incompleta ovvero ritenga necessario integrare la documentazione*” ad essa allegata. Il diniego all'iscrizione, comunque, non impedisce di inviare una nuova comunicazione (art. 3, comma 7).

La sezione speciale del registro dei cambiavalute sarà istituita entro 90 giorni dall'entrata in vigore del Decreto da parte dell'OAM che ne cura “*la chiarezza, la completezza e l'accessibilità al pubblico dei dati*” e dispone di poteri di sospensione e cancellazione dal Registro medesimo (art. 4, commi 1, 2 e 5). Quest'ultimo riporta i dati relativi al Prestatore di servizi e alla tipologia di attività svolta (meglio descritta nell'Allegato 2 al Decreto), i punti fisici di

operatività e/o l'indirizzo web tramite cui è offerto il servizio relativo all'utilizzo di valuta virtuale e di portafoglio digitale (art. 4, comma 3).

Trimestralmente, i Prestatori di servizi iscritti al Registro devono comunicare all'OAM i dati dei loro clienti e delle operazioni effettuate per loro conto, come specificati nell'Allegato 1 al Decreto (art. 5).

Semestralmente, inoltre, anche sulla base delle informazioni trasmesse ex art. 5 del Decreto, l'OAM deve inviare al Ministero dell'economia e delle finanze una relazione contenente: 1) il numero di soggetti che hanno trasmesso la comunicazione per l'iscrizione al Registro, anche se non l'abbiano poi ottenuta; 2) la tipologia di servizi prestati dagli iscritti; 3) le ipotesi di esercizio abusivo dell'attività; 4) i dati aggregati trasmessi dai Prestatori di servizi all'OAM sulle operazioni da essi effettuate (art. 3, comma 8).

Ai sensi del combinato disposto degli artt. 4, comma 4 e 6, comma 1 del Decreto, l'OAM collabora coi soggetti di cui all'art. 21, comma 2 D. Lgs. 231/07 fornendogli *“tempestivamente”*, su richiesta, ogni informazione e documento riguardante i Prestatori di servizi *“detenuta in forza della gestione della sezione speciale del registro”*, ivi compresi i dati trasmessi all'OAM ex art 5 del Decreto. I soggetti di cui all'art. 21, comma 2 D. Lgs. 231/07 includono: Ministero dell'economia e delle finanze, Autorità di vigilanza di settore, Unità di Informazione Finanziaria per l'Italia, Direzione investigativa antimafia, Guardia di finanza che operi tramite il Nucleo Speciale di Polizia Valutaria.

Le forze di polizia che rilevino l'esercizio abusivo di servizi relativi all'utilizzo di valuta virtuale o di portafoglio digitale possono accertare e contestare la violazione ai sensi della L. n. 689/81 (art. 6, comma 2).

Per quanto qui interessa, infine, occorre dare atto che il 18 febbraio 2022 l'OAM ha diffuso un comunicato stampa con cui sostanzialmente riassume i contenuti del Decreto e, soprattutto, informa che la sezione speciale del registro dei cambiavalute sarà attivata entro il 18 maggio 2022.

EMANUELE STABILE

[https://www.gazzettaufficiale.it/atto/serie\\_generale/caricaDettaglioAtto/originario?atto.d\\_ataPubblicazioneGazzetta=2022-02-17&atto.codiceRedazionale=22A01127&elenco30giorni=true](https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.d_ataPubblicazioneGazzetta=2022-02-17&atto.codiceRedazionale=22A01127&elenco30giorni=true)

2022/1(8)GDI

### **La decisione del 10 febbraio 2022 del garante privacy italiano sul trattamento di dati biometrici da parte di Clearview AI**

Dopo la CNIL, l'autorità di controllo francese, che il 16 dicembre 2021 ha dichiarato illecito il trattamento di dati personali effettuato dalla società Clearview AI e imposto la cessazione della raccolta e trattamento di dati personali sul territorio francese, anche l'autorità italiana, il Garante per la protezione dei dati personali (di seguito il **“Garante”**), è intervenuto con provvedimento in data 10 febbraio 2022 accertando l'illiceità della raccolta di dati biometrici operata dalla medesima società e comminando una sanzione pecuniaria di 20 milioni di euro. In precedenza, Clearview AI era stata assoggettata ad un analogo provvedimento in Germania, sia pure relativamente al trattamento dei dati biometrici di una sola persona, il Sig. Matthias Marx (provvedimento del 27 gennaio 2021 dell'autorità per la protezione dei dati personali della città di Amburgo, su cui v. la notizia [2021/1\(8\)CR](#)).

Clearview AI è una società statunitense, costituita nel 2017, che ha creato un motore di ricerca di immagini, all'interno di un proprio database, tramite riconoscimento facciale. A tal fine, la società raccoglie, attraverso tecniche di *web scraping*, immagini da social network, blog e siti web in cui sono presenti foto o video liberamente accessibili che vengono elaborati con tecniche biometriche al fine di estrarre le caratteristiche identificative del volto di ogni persona ritratta per consentirne l'indicizzazione e la successiva ricerca. Clearview ottiene così profili basati sui dati biometrici estratti dalle immagini, eventualmente arricchiti da altre informazioni ad esse correlate come titolo, geolocalizzazione della foto o pagina web di pubblicazione, consentendole di offrire un servizio di ricerca delle persone. La piattaforma è dichiaratamente stata creata al fine di fornire un servizio di ricerca biometrica altamente qualificata.

Diversamente da quanto affermato dalla società, che non si riteneva soggetta al GDPR (il Regolamento UE 2016/679, di seguito il “**Regolamento**”) in quanto avente sede legale negli USA e perché dichiarava di non offrire i propri servizi a cittadini europei, il Garante ha accertato che la stessa ha invece trattato i dati anche di cittadini italiani e di persone collocate in Italia. Inoltre, mentre la società ha sostenuto di non tracciare né monitorare le persone nel tempo, ma di eseguire una forma di classificazione che si risolverebbe in un'istantanea dei risultati della ricerca al momento del compimento della stessa, il Garante ha constatato invece la realizzazione di una comparazione tra immagini idonea ad integrare un'attività assimilabile al controllo del comportamento dell'interessato in quanto posta in essere tramite il tracciamento in internet e la successiva profilazione.

Il Garante ha accertato inoltre l'illiceità del trattamento dei dati personali detenuti dalla società, inclusi quelli biometrici e di geolocalizzazione, in quanto effettuato senza un'adeguata base giuridica respingendo la tesi della difesa secondo la quale il trattamento si poteva basare sul legittimo interesse.

Secondo il Garante, la società ha poi violato altri principi del Regolamento come: quelli relativi agli obblighi di trasparenza, non avendo adeguatamente informato gli interessati; quello di limitazione delle finalità del trattamento, avendo utilizzato i dati per scopi diversi rispetto a quelli per i quali erano stati pubblicati online; e quello di limitazione della conservazione, non avendo stabilito tempi di conservazione dei dati.

Conseguentemente, il Garante ha rilevato la violazione degli artt. 5, par. 1, lett. a), b) ed e), 6, 9, 12, 13, 14, 15 e 27 del Regolamento e comminato una sanzione amministrativa di 20 milioni di euro oltre al divieto di prosecuzione del trattamento, l'ordine di cancellare i dati relativi a persone che si trovano in Italia, nonché quello di designare un rappresentante nel territorio dell'Unione europea che funga da interlocutore, in aggiunta o in sostituzione del titolare con sede negli Stati Uniti, al fine di agevolare l'esercizio dei diritti degli interessati.

GUIDO D'IPPOLITO

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9751362>

2022/1(9)CR

### **La decisione del 13 gennaio 2022 del garante privacy austriaco sul trasferimento di dati personali negli USA da parte di Google Analytics**

Il 13 gennaio 2022 l'autorità garante per la protezione dei dati austriaca (“**Datenschutzbehörde**” o “**DSB**”) si è pronunciata sulla legittimità dell'utilizzo di Google

Analytics. La decisione deve essere letta alla luce della sentenza “Schrems II” con cui a luglio 2020 la Corte di Giustizia dell’UE aveva dichiarato illegittimo il *Privacy Shield* in quanto gli Stati Uniti non garantivano un livello di protezione dei dati personali equivalente a quello riconosciuto nell’UE dal GDPR (su cui v. la notizia [2020/3\(1\)CR](#)). In seguito alla decisione della Corte, ad agosto 2020, il gruppo Noyb - fondato dallo stesso Schrems - aveva presentato 101 reclami davanti alle autorità garanti di diversi Stati Membri contro società che trasferivano dati personali verso gli USA attraverso Google Analytics e/o Facebook Connect integrations.

L’autorità austriaca è stata la prima a pronunciarsi su uno di questi reclami con riferimento ad un sito web che trasferiva i dati degli utenti negli Stati Uniti attraverso l’utilizzo di Google Analytics. Il DSB ha ritenuto che il trattamento dei dati personali effettuato attraverso Google Analytics violi il Capo V del GDPR in quanto i dati personali sono trasferiti verso un Paese extra UE - gli USA - che non garantisce un livello di protezione equivalente a quello assicurato dalla normativa europea sulla protezione dei dati. Questo, in particolare, a causa della possibilità per le autorità statunitensi di accedere ai dati detenuti da Google e di identificare l’utente interessato. Anche l’uso di *Anonymize IP* (il servizio di Google Analytics che permette di rimuovere le prime cifre dell’indirizzo IP, rendendolo così non più associabile all’utente) è stato considerato dall’autorità irrilevante, in quanto l’indirizzo IP è solo “un pezzo del puzzle” e Google può utilizzare altri dati in suo possesso per riuscire ad individuare l’utente. Sia le Clausole Contrattuali Standard (di cui Google si è servita in seguito all’invalidamento del *Privacy Shield*) che le misure supplementari (contrattuali, organizzative e tecniche) adottate da Google per rendere il trasferimento dei dati conforme al GDPR sono state ritenute insufficienti. Infatti, a detta del DBS, qualsiasi misura supplementare può essere considerata efficace solo se affronta le carenze specifiche individuate nella valutazione della situazione nel paese terzo, vale a dire in questo caso le possibilità di accesso e di sorveglianza da parte dei servizi segreti statunitensi. Tuttavia, le misure contrattuali di per sé non hanno efficacia vincolante nei confronti delle autorità del paese terzo, per cui devono essere integrate con ulteriori misure. La stessa crittografia non è stata considerata una misura adeguata in quanto se il *provider* possiede la chiave (come nel caso di Google), in caso di richiesta di accesso da parte delle autorità statunitensi potrà essere obbligato a rivelare tale chiave insieme ai dati, vanificando così di fatto la relativa protezione.

Questa decisione avrà probabilmente un profondo impatto sul tema del trasferimento dei dati personali verso gli Stati Uniti che, dopo più di un anno dalla sentenza “Schrems II”, non ha ancora avuto sviluppi significativi. Nonostante l’annullamento del *Privacy Shield*, infatti, le società europee hanno di fatto continuano ad avvalersi di *provider* i cui *server* si trovano negli USA o che, comunque, sono soggetti alla legge statunitense. In particolare, Google Analytics rimane oggi la piattaforma di *web analytics* maggiormente utilizzata dai *website owner* e difficilmente sostituibile. D’altra parte, è evidente come il problema del trasferimento dei dati verso gli USA vada ben oltre i singoli titolari, nonché le stesse *big tech*. Si tratta, infatti, di un problema principalmente politico che richiede necessariamente una soluzione a monte attraverso il raggiungimento di un accordo tra la Commissione Europea e il Governo statunitense.

CHIARA RAUCCIO

[https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics\\_EN\\_bk.pdf](https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_EN_bk.pdf)

2022/1(10)CR

### **La decisione del 10 febbraio 2022 del garante privacy francese sul trasferimento di dati personali negli USA da parte di Google Analytics**

Dopo la pronuncia dell'autorità austriaca, anche l'autorità garante della protezione dei dati personali francese (“*Commission Nationale de l'Informatique et des Libertés*” o “**CNIL**”) il 10 febbraio 2022 è intervenuta sul tema del trasferimento dei dati personali verso gli Stati Uniti attraverso Google Analytics. Anche in questo caso l'autorità si è pronunciata in seguito ad un reclamo presentato da Noyb (associazione fondata da Schrems) sulla base della sentenza “Schrems II” con cui a luglio 2020 la Corte di Giustizia dell'UE ha invalidato il *Privacy Shield*. La decisione del CNIL si pone sulla scia di quella adottata poco più di un mese prima dall'omologa autorità austriaca, confermando così l'atteggiamento unitario adottato dalle *Data Protection Authority* (“**DPA**”) europee sul tema del trasferimento dei dati personali verso gli USA.

Il CNIL ha innanzitutto esaminato il funzionamento di Google Analytics e le modalità con cui avviene il trasferimento dei dati personali. Google Analytics – il servizio di *web analytics* ad oggi più utilizzato a livello globale - può essere integrato nei siti web per misurare in termini statistici il numero di utenti che visitano la pagina. Per fare ciò ad ogni visitatore viene associato un identificatore univoco. Tuttavia, nonostante l'analisi sia aggregata e l'identificatore sia tenuto separato dai dati identificativi dell'utente, l'identificatore costituisce comunque un dato personale in quanto Google, combinandolo con altri dati in suo possesso, rimane in grado di associarlo ad una persona fisica determinata.

Conseguentemente, il trasferimento verso gli Stati Uniti degli identificatori e delle informazioni relative alle interazioni degli utenti ad essi associati pone un tema di legittimità del trasferimento ai sensi della normativa UE in materia di protezione dei dati personali. Nello specifico il CNIL ha ribadito che, in seguito alla sentenza Schrems II e all'assenza di una nuova decisione di adeguatezza, il trasferimento dei dati verso gli USA può avvenire solo sulla base di adeguate garanzie. Tuttavia, secondo l'autorità francese – come del resto già sostenuto dall'autorità austriaca – le misure supplementari poste in essere da Google non sono sufficienti a garantire un livello di protezione adeguato. La *parent company* di Google (Alphabet Inc.), infatti, rientra tra gli operatori economici soggetti alle leggi di sorveglianza degli Stati Uniti, con la conseguenza che i servizi segreti statunitensi hanno *ex lege* la facoltà di accedere ai dati acquisiti tramite il servizio Analytics. Alla luce di ciò le misure di sicurezza adottate da Google, non avendo efficacia vincolante nei confronti delle autorità di sorveglianza statunitensi, non sono in grado di impedire l'accesso ai dati da parte dei servizi di *intelligence* e, dunque, non eliminano il rischio per gli utenti europei dei siti web che utilizzano il servizio. Ne consegue che il trasferimento ad oggi effettuato attraverso Google Analytics viola le disposizioni del Capo V del GDPR ed è, dunque, illegittimo.

Il CNIL non ha irrogato una sanzione al sito web oggetto del provvedimento, ma ha concesso un mese di tempo per porre fine alla violazione interrompendo l'utilizzo di Google Analytics, se necessario, o utilizzando un servizio che non implichi il trasferimento dei dati verso gli Stati Uniti. Al riguardo il CNIL ha raccomandato di utilizzare solo strumenti che producano dati statistici anonimi, così da evitare trasferimenti illegali, e ha avviato un piano di valutazione per determinare quali soluzioni sul mercato consentano di non raccogliere il consenso dell'interessato.

In ogni caso la decisione in esame risulta di particolare rilievo in quanto conferma la posizione intransigente assunta dalle DPA europee rispetto ai trasferimenti di dati verso gli Stati Uniti, evidenziando nuovamente l'esigenza sempre più pressante di una soluzione.

CHIARA RAUCCIO

<https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply>

2022/1(11)VR

### **La decisione del 2 febbraio 2022 del garante privacy belga sul Real Time Bidding e le attività di online advertising a proposito del Quadro di Trasparenza e Consenso elaborato e gestito da IAB Europe**

Il 2 febbraio 2022 la *Litigation Chamber* del Garante per la protezione dei dati personali belga (“**Garante Privacy**” o “**Autorità**”), quale organo amministrativo di risoluzione delle controversie, ha dichiarato l’illegittimità dei trattamenti di dati su larga scala effettuati dalla *Interactive Advertising Bureau Europe* (“**IAB Europe**”) in quanto violativi di numerose disposizioni del GDPR, comminando relative sanzioni, di seguito illustrate.

Nello specifico, l’oggetto del provvedimento è duplice, concernendo, *in primis*, la conformità al GDPR del *Transparency & Consent Framework* (“**TCF**”) predisposto e gestito da IAB Europe e, conseguentemente, il suo impatto sul c.d. *Real-Time Bidding* (“**RTB**”).

Il settore della pubblicità online opera “dietro le quinte” delle pagine web, attraverso metodi di c.d. “*Programmatic advertising*” tra cui primeggia l’offerta in tempo reale (RTB), definita in letteratura come rete di partner che permette applicazioni di *big data* per migliorare le vendite di spazi pubblicitari predeterminati attraverso il *marketing* guidato dai dati in tempo reale e la pubblicità (comportamentale) personalizzata. Si tratta, in sostanza, di un sistema di aste virtuali istantanee e automatizzate tramite algoritmi, attraverso cui si realizza l’interscambio di offerte d’acquisto di spazi pubblicitari personalizzati. Come minutamente illustrato dall’Autorità, il RTB coinvolge: *i*) le imprese che gestiscono il sistema e ne delineano le politiche, la *governance* e i protocolli tecnici; *ii*) dal lato dell’offerta, le imprese che possiedono siti web o applicazioni con disponibilità di spazi pubblicitari (“*publishers*”) e quelle che gestiscono piattaforme online automatizzate sulle quali i *publishers* registrati possono segnalare la disponibilità dei propri spazi pubblicitari, sollecitandone la domanda (“*Sell-Side Platforms*” o “SSP”); *iii*) dal lato della domanda, gli inserzionisti e le imprese che gestiscono piattaforme di ottimizzazione della richiesta di spazi pubblicitari (“*Demand-Side Platforms*” o “DSPs”); *iv*) intermediari che veicolano gli scambi, viepiù consentendo alle DSP di emettere offerte parametrizzate sulle richieste avanzate dalle SSP (“*Ad Exchanges*”); *v*) le cc.dd. “*Data Management Platforms*” (“DMP”), che estraggono ingenti quantità di dati personali di vario tipo da molteplici fonti (dispositivi, *cookies*, identificatori mobili, analisi comportamentali, *social media*, dati offline ecc.), per poi centralizzarli, analizzarli e classificarli mediante algoritmi, fornendo così profili dettagliati dei consumatori per l’ottimizzazione del *targeting* e la personalizzazione delle offerte. La dinamica è, in estrema sintesi, la seguente: dopo aver elaborato profili dettagliati di consumatori tramite una DMP, gli inserzionisti emettono offerte tramite le DSP per intercettare la disponibilità dei pertinenti spazi pubblicitari dei *publishers* segnalati via SSP; perciò, non appena l’utente accede a una pagina web: i *publishers* interessati selezionano una SSP; questa seleziona un *Ad exchange*; esso invia richieste di offerte a centinaia di partner della

rete, invitandoli a rispondere, e piazza l'offerta maggiore; infine, la DSP presenta l'annuncio dell'inserzionista vincitore.

Così delineato, il RTB, anche per dimensione e numero di operatori coinvolti, presenta rischi seri e fisiologici, tra cui: la profilazione e il processo decisionale automatizzato; il trattamento su larga scala anche di categorie speciali di dati, uso innovativo o applicazione di nuove soluzioni tecnologiche o organizzative; abbinamento o fusione di *datasets*; analisi o previsione del comportamento, della posizione o dei movimenti delle persone fisiche; trattamenti non trasparenti.

Fra i protocolli maggiormente utilizzati a livello mondiale per il RTB vi sono il sistema "OpenRTB", assieme all'associato "*Advertising Common Object Model*" (AdCOM), sviluppati da IAB *Technology Laboratory Inc.* ("IAB Tech Lab") e *Interactive Advertising Bureau Inc.* ("IAB"), e il sistema di "acquirenti autorizzati" "AdBuyers", sviluppato da Google. Entità affatto distinta è IAB Europe, federazione rappresentativa di circa 5000 imprese e associazioni nazionali operanti nel ramo della pubblicità e del marketing digitale, cui si deve la paternità del TCF, ossia l'insieme di politiche, specifiche tecniche, termini e condizioni proposte come standard di *best practice* intersettoriale asseritamente idoneo ad assicurare la conformità dell'industria della pubblicità digitale con la regolazione UE in materia di protezione dei dati personali. Perciò, ferma la distinzione ontologica tra TCF e OpenRTB, essi sono fatalmente destinati a intersecarsi, giacché – come affermato da IAB Europe – il primo fornisce un quadro operativo di allineamento al GDPR dei trattamenti svolti sulla base del secondo. Inoltre, se vi è larga coincidenza fra gli attori dei due sistemi, una peculiarità del TCF è la presenza delle cc.dd. "*Consent Management Platforms*" ("CMPs"), consistenti in *pop-up* mostrati all'atto della prima connessione a un sito web per raccogliere il consenso dell'utente al posizionamento di *cookie* e altre informazioni identificative. Ebbene, parte essenziale dell'intervento delle CMP è la generazione di una stringa composta da una combinazione di lettere, numeri e altri caratteri, denominata "*Transparency and Consent String*" ("TC String"), volta all'acquisizione automatica di preferenze dell'utente quali: il consenso o meno al trattamento dei dati personali per scopi di *marketing* o altri, la condivisione o meno dei dati con terze parti venditori e l'esercizio o meno del diritto di opposizione. In estrema sintesi, la TC String viene decifrata dai cc.dd. "*Adtech vendors*" (inserzionisti, SSP, DSP, *Ad Exchanges* e DMP) per determinare la sussistenza della base giuridica necessaria a trattare i dati personali di un utente.

Ciò premesso, l'esame della *Litigation Chamber* ha ad oggetto esclusivamente il trattamento di dati personali all'interno del TCF e le relative responsabilità, affrontando solo *per incidens* le attività compiute nel sistema OpenRTB e i relativi rischi.

Anzitutto, l'Autorità dichiara che le preferenze degli utenti raccolte nella TC String costituiscono tecnicamente dati personali. Infatti, tanto la legislazione UE (cfr. art. 4, paragrafo 1 GDPR e art. 2.a Convenzione di Strasburgo del 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale) quanto la giurisprudenza della CGUE adottano un concetto ampio di dato personale, al fine di garantire un elevato livello di tutela degli interessati. Costituisce dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o (indirettamente) per mezzo di identificatori ai quali l'utente può essere collegato attraverso i suoi dispositivi, applicazioni, strumenti e protocolli, come gli indirizzi IP, i *cookie* di identificazione o altri (cfr. considerando n. 30 GDPR). In altri termini, ove determinate informazioni possono essere associate a una persona identificata o identificabile tramite i mezzi che possono ragionevolmente impiegarsi, esse devono qualificarsi come dati personali. Ebbene, nonostante sia pacifico che la TC String, a ragione della limitatezza e del carattere delle informazioni *in vi* contenute, non consente un'identificazione diretta dell'interessato,

quest'ultimo è certamente identificabile. Infatti, i *pop-up* di consenso predisposti e gestiti dalle CMP elaborano inevitabilmente anche l'indirizzo IP dell'utente, il quale diviene così agilmente associabile alle preferenze raccolte nella stringa memorizzata o letta dalla stessa CMP. In sostanza, è proprio la possibilità di associare le TC String agli indirizzi IP a rendere identificabile l'interessato. Ne consegue non solo che IAB Europe dispone di mezzi ragionevoli per l'identificazione degli utenti ma financo che ciò, a ben vedere, parrebbe essere lo scopo ultimo delle operazioni effettuate nell'ambito del *framework*. Una volta chiarita la natura di dati personali delle preferenze degli interessati, deve concludersi anche che il quadro del TCF presuppone fisiologicamente il trattamento degli stessi ai sensi dell'art. 4.2. GDPR, ponendosi come approccio standardizzato per la raccolta, l'elaborazione, l'archiviazione e la successiva condivisione delle preferenze degli utenti.

Ai fini dell'attribuzione di responsabilità in capo a IAB Europe, questione preliminare è poi la sua qualificabilità come titolare del trattamento *ex art. 4.7* GDPR. Anche tale nozione è piuttosto ampia, al precipuo scopo di ricomprendervi le entità che esercitano un controllo effettivo sulle operazioni di trattamento, determinandone, singolarmente o insieme ad altri, le finalità e i mezzi. Inoltre, come chiarito dal Comitato europeo per la protezione dei dati (lo "EDPB"), tale influenza può esercitarsi anche tramite poteri impliciti o di fatto. In quest'ottica, diviene cruciale il ruolo funzionale che un operatore assume: dalla giurisprudenza si apprende infatti che non è necessario un accesso diretto ai dati personali né tantomeno che il trattamento sia effettuato in prima persona, essendo sufficiente l'esercizio di un'influenza decisiva sul "perché" e sul "come" di tali operazioni. Il TCF, beninteso, non integra di per sé un trattamento; e tuttavia, come *supra* illustrato, esso integra un quadro di politiche e specifiche tecniche vincolanti nel cui contesto i trattamenti si strutturano di fatto sulle linee elaborate da IAB Europe. In particolare, l'accettazione dei *Terms and Conditions* da parte degli *Adtech vendors* obbliga quest'ultimi a osservare regole predefinite per il trattamento delle TC String nel TCF. In quest'ottica, dalla documentazione redatta da IAB Europe emerge anzitutto che gli scopi della TC String e, *amplius*, del suo trattamento nell'ambito del TCF sono determinati puntualmente da IAB Europe mediante un elenco tassativo. Inoltre, quest'ultima individua e prescrive anche i mezzi essenziali – quelli cioè strettamente legati allo scopo e alla portata del trattamento (cfr. EDPB - *Guidelines 7/2020 on the concepts of controller and processor in the GDPR*, v2.0, 2021, par. 39-41) – per l'elaborazione della TC String. Ad esempio, le politiche, le specifiche tecniche e le linee guida di attuazione del TCF precisano che le CMP, nel raccogliere il consenso degli utenti, debbano generare una stringa unica e memorizzarne il valore. Per far ciò, sono obbligati a registrarsi presso IAB Europe e a seguire le specifiche tecniche, sviluppate in collaborazione con IAB Tech Lab, attinenti all'API132, con cui la stringa può essere generata e letta da *publishers* e *Adtech vendors*. Le medesime regole ne individuano altresì il contenuto, specificando le informazioni incluse. In generale, IAB Europe determina di fatto le modalità di generazione, conservazione e condivisione della TC String, con cui vengono trattate le preferenze, le obiezioni e il consenso degli utenti. Ne consegue che IAB Europe deve senz'altro qualificarsi come titolare del trattamento ai sensi dell'art. 4, paragrafo 7 GDPR.

Per inciso, quanto sopra non implica che la titolarità dei trattamenti, e la conseguente responsabilità, sia esclusivamente di IAB Europe. All'opposto, l'Autorità ritiene configurabile un'ipotesi di contitolarità *ex art. 26* GDPR con le CMP, i *publishers* e gli *Adtech vendors*, avendosi di fatto una determinazione congiunta delle finalità e dei mezzi. Naturalmente, la misura delle responsabilità individuali è variabile in base alla concreta entità e alla fase di coinvolgimento del singolo attore, essendo necessaria solamente una convergenza di decisioni in modo che ne sia provata una tangibile mutua influenza. Al riguardo, a ben vedere, IAB Europe realizza, col TCF, un sistema all'interno del quale il

consenso, le obiezioni e le preferenze degli utenti sono raccolti e scambiati non per i propri scopi o per la propria conservazione, bensì per agevolare l'ulteriore trattamento da parte di terzi qualificati.

Passando all'esame delle violazioni del GDPR, l'Autorità muove dalla liceità e correttezza del trattamento. Ai fini della verifica di compatibilità con gli artt. 5, paragrafo 1 e 6 GDPR, vengono distinte preliminarmente: *a)* le attività di acquisizione del consenso, delle obiezioni e delle preferenze degli utenti nella TC String da parte delle CMP; *b)* la raccolta e la diffusione dei dati personali degli utenti nel protocollo OpenRTB da parte delle imprese partecipanti al TCF.

Ferma la qualificabilità delle operazioni di generazione e diffusione della TC String come trattamenti di dati, se ne indaga dunque la base giuridica. Né le politiche né le linee guida del TCF prevedono un obbligo per le CMP di ottenere il consenso inequivocabile degli utenti prima di acquisire le loro preferenze nella stringa. A ciò si accompagna un rilevante difetto di informazione, poiché l'utenza non è posta a conoscenza dell'esistenza stessa dei trattamenti, dei soggetti con cui vengono condivise le loro preferenze, né i tempi di conservazione delle stesse: l'art. 6, lett. *a)* GDPR non è quindi applicabile. Del pari, non è invocabile la lett. *b)*, difettando il requisito dell'obiettiva necessità del trattamento alla fornitura di servizi online da parte dei *publishers* agli utenti interessati, sempre ammesso che sussista a monte un effettivo rapporto contrattuale. Per tali ragioni, l'analisi si incentra sull'art. 6, lett. *f)*, ossia sulla sussistenza di un interesse legittimo del titolare del trattamento o di terzi, debitamente bilanciato con gli interessi o i diritti e le libertà fondamentali degli interessati. Com'è noto, il requisito *de quo* richiede il cumulo di tre condizioni analiticamente indicate dalla giurisprudenza della CGUE (sentenza Rigas, 11 dicembre 2009, C-708/18), dovendosi dimostrare che: gli interessi perseguiti col trattamento siano riconosciuti come legittimi (“*test dello scopo*”); che il trattamento sia necessario per il perseguimento dell'interesse legittimo (“*test di necessità*”); non siano lesi diritti e libertà fondamentali dell'interessato (“*test del bilanciamento*”). Ebbene, la *Litigation Chamber* ritiene che le prime due verifiche abbiano esito positivo, dal momento che l'acquisizione del consenso e delle preferenze degli utenti, come parte essenziale del TCF, integra un interesse legittimo di IAB Europe e degli *Adtech vendors* coinvolti e i dati personali inclusi nella TC String sono limitati a quanto strettamente necessario a tale scopo. Per quanto concerne il terzo test, il considerando n. 47 GDPR impone che il bilanciamento tenga conto delle ragionevoli aspettative degli interessati, dovendosi valutare se questi, al momento e nel conteso concreto in cui avviene la raccolta dei dati, potevano prefigurarsi un trattamento degli stessi per il perseguimento dell'interesse legittimo debitamente esplicitato *ex art.* 5, lett. *b)* GDPR. Il quadro fattuale dimostra l'assenza di possibilità per gli utenti di opporsi *in toto* ai trattamenti effettuati nel contesto del TCF, essendo automatica la generazione della stringa da parte delle CMP e il suo collegamento all'ID unico dei singoli interessati attraverso un *cookie euconsent-v2* posto sui loro dispositivi. L'esito negativo del *balancing test* impedisce dunque l'invocabilità dell'art. 6, lett. *f)*, da cui discende fatalmente la declaratoria di violazione degli artt. 5, paragrafo 1 e 6 GDPR per mancanza di una valida base giuridica dei trattamenti condotti nell'ambito del TCF.

Per quanto concerne la raccolta e la diffusione dei dati personali degli utenti nel contesto del protocollo OpenRTB da parte delle imprese partecipanti al TCF, la base giuridica di tali operazioni non può ritenersi offerta dall'art. 6, lett. *a)*, poiché il consenso ottenuto dalle CMP non soddisfa i requisiti dell'art. 7 GDPR. Esso, infatti, non risulta sufficientemente libero, specifico, informato e non ambiguo. Anzitutto, alcune le finalità di trattamento indicate da IAB Europe nelle politiche del *framework*, come la “misurazione della performance dei contenuti” o la “applicazione di ricerche di mercato per generare previsioni sul pubblico”, sono intrasparenti e financo decettive, non fornendo informazioni sull'ambito del

trattamento, sulla natura dei dati i trattati o sulle tempistiche di conservazione. Inoltre: l'interfaccia utente delle CMP non fornisce una panoramica delle categorie di dati raccolti; risulta particolarmente ostico per gli utenti ottenere maggiori informazioni sull'identità dei soggetti coinvolti come contitolari dei trattamenti, difficoltà acuita dall'ingente numero di attori, che rende di fatto impossibile un consenso realmente informato; infine, il consenso, una volta ottenuto dalle CMP, non può essere ritirato dagli utenti con la stessa facilità con cui è prestato, non avendosi alcuna misura per impedire agli *Adtech vendors* di proseguire le operazioni avviate sulla base del consenso iniziale. Ciò chiarito, il *focus* non può che spostarsi sull'art. 6, lett. f), indagando se e fino a che punto possa intravedersi un legittimo interesse a fondamento del *target advertising* e della profilazione. In questo caso, il triplice test rivela un esito ancor più negativo. Difatti, la genericità delle finalità di trattamento rende ardua la valutazione di necessità delle menzionate operazioni, non consentendo di rinvenire una base giuridica sufficientemente specifica, esistente, attuale e non ipotetica. A ben vedere, infatti, le politiche TCF non contemplano un obbligo per le CMP di esplicitare i legittimi interessi, prescrivendo requisiti specifici per l'interfaccia utente (UI) circoscritti a un livello meramente secondario di informazioni. Non solo. Nonostante si discorra di requisiti minimi, il TCF dispone che l'UI contenga esclusivo riferimento alle definizioni degli scopi pubblicati nel testo legale standard, cui è attribuito carattere "definitivo". Perciò, l'interpretazione della *Litigation Chamber* è nel senso che tali regole proibiscono di fatto alle CMP di fornire ulteriori informazioni agli interessati tanto in merito agli interessi legittimi perseguiti quanto al bilanciamento con i diritti e le libertà fondamentali dell'utente. In sostanza, dunque, il test dello scopo non può dirsi superato. Analogamente deve dirsi per il test di necessità, mancando adeguate garanzie che i dati raccolti e diffusi siano limitati a quanto strettamente necessario per le finalità previste. Infine, l'elevato numero di attori operanti nel TCF non consente agli interessati di sviluppare ragionevoli aspettative ai sensi del considerando n. 47 GDPR, dovendo escludersi un acconcio bilanciamento. Per completezza, si aggiunge che il TCF non contempla, per le ipotesi in questione, alcun riferimento alla necessità contrattuale come base giuridica *ex art. 6, lett. b) GDPR*.

L'esame in merito alle asserite violazioni del GDPR prosegue con riferimento ai presidi di trasparenza prescritti agli artt. 12, 13 e 14 del regolamento. In proposito, si rileva preliminarmente come le politiche del TCF attribuiscono in certi casi a IAB Europe il potere di reclamare le registrazioni del consenso che le CMP sono tenuti a conservare, omettendo però di prevedere un correlativo obbligo di informazione circa tale possibile trattamento. Ma soprattutto, il numero di *Adtech vendors* potenzialmente coinvolti nel ricevere e trattare ulteriormente i dati degli utenti sulla base delle preferenze da essi prestate, unita all'echeggiata genericità di alcune delle finalità dichiarate, non consente di ritenere soddisfatto il requisito di una forma trasparente, intellegibile e facilmente accessibile di cui all'art. 12.1 GDPR, con particolare enfasi sulla grave assenza di quell'elemento di concisione sul quale già il "Gruppo 29" insisteva per evitare un "affaticamento informativo" (WP 260 – *Guidance on transparency under the GDPR*, par. 8). Per tali ragioni, l'Autorità ritiene che il TCF violi le condizioni di trasparenza richieste dagli artt. 12, 13 e 14 GDPR.

Infine, è analizzata la compatibilità del quadro TCF con i principi di responsabilità (art. 24 GDPR), protezione dei dati fin dalla progettazione e per impostazione definita (Art. 25 GDPR), integrità e riservatezza (art. 5.1 GDPR) e sicurezza nel trattamento (art. 32 GDPR). Com'è noto, l'art. 24 impone al titolare del trattamento di approntare misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento (con obbligo di riesame e aggiornamento), in ciò riflettendo l'art. 5.2. Inoltre, in consonanza col considerando n. 74, le misure *de quibus* devono tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del

trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Ai sensi dell'art. 32, poi, il titolare e il responsabile devono mettere in atto misure tecniche e organizzative per garantire un livello di sicurezza del trattamento adeguato al rischio. Si tratta di un punto di grande importanza, che si lega a doppio filo coi principi di integrità e riservatezza e i conseguenti obblighi di sicurezza dei dati e di protezione mediante misure tecniche e organizzative adeguate di cui all'art. 5, lett. *f*). Infatti, in assenza di opportuni presidi in tal senso, spiega l'Autorità, il rispetto dei diritti fondamentali non può essere efficacemente assicurato, vieppiù in considerazione del ruolo cruciale svolto dalle tecnologie dell'informazione e della comunicazione nella nostra società. In altri termini, dato l'altissimo numero di TC String generate quotidianamente in seno al TCF, è essenziale che le norme che ne regolano la partecipazione siano osservate da tutte le parti coinvolte e che tale osservanza sia supervisionata da IAB Europe in qualità di *"Managing Organisation"*. Tuttavia, sono le stesse politiche redatte da IAB Europe a prendere in considerazione l'ipotesi che, difettando un sistema di convalida, le CMP possano falsificare o modificare le TC String e, precisamente, i segnali generativi del *cookie euconsent-v2*, riproducendo consensi "falsi", non effettivamente (o comunque, non validamente) prestati dagli interessati. Che le misure di controllo offerte nel TCF siano insufficienti lo rivela anche il c.d. *"TCF Vendor Compliance Programme"*, ove, a fronte di declamatori incoraggiamenti a garantire la sicurezza dei trattamenti, difetta un monitoraggio sistematico da parte di IAB Europe. Infine, il citato programma contempla un sistema sanzionatorio scarsamente dissuasivo, potendo, ad esempio, un venditore dichiararsi responsabile di una violazione fino a tre volte, prima di ricevere un termine di ventotto giorni per conformarsi, alla scadenza del quale sarà rimosso (peraltro non irreversibilmente) dalla *Global Vendors List*. In conclusione, dunque, la *Litigation Chamber* ascrive in capo a IAB Europe una responsabilità per violazione dell'obbligo di garantire la sicurezza, l'integrità e la riservatezza dei trattamenti.

Per completezza, si compendiano alcuni rilievi finali in merito ad ulteriori asserite violazioni del GDPR. *In primis*, la limitata entità dei dati sul singolo utente memorizzati nelle TC String porta a escludere una violazione dei principi di limitazione delle finalità e di minimizzazione dei dati (art. 5, lett. *b*) e *c*) GDPR) nel contesto della TCF, potendosi quest'ultima verificare solo in seno al protocollo OpenRTB, rispetto al quale però IAB Europe non agisce come titolare dei trattamenti. Inoltre, non è provata la conservazione delle TC String e la relativa memorizzazione dei dati personali per periodi di tempo non autorizzati, in violazione dell'articolo 5, lett. *e*) GDPR. Di particolare importanza è il rilievo che le TC String non contengono in sé informazioni tali da poter estrarre – neanche indirettamente, rendendo ad esempio accessibile la cronologia dei siti web visitati dall'interessato – categorie particolari di dati personali *ex* art. 9 GDPR. Risultano invece violati: l'art. 30 GDPR sulla tenuta dei registri delle attività di trattamento, per mancanza di riferimenti ai segnali di consenso, alle obiezioni e alle preferenze degli utenti; l'obbligo di effettuare la valutazione di impatto sulla protezione dei dati *ex* art. 35; l'obbligo di nominare un DPO ai sensi dell'art. 37.

In considerazione dei suesposti rilievi, l'Autorità, al fine di rendere il trattamento dei dati personali nell'ambito del TCF conforme alle disposizioni del GDPR, adotta gli ordini di conformità, i divieti e commina le sanzioni che seguono. A IAB Europe è ordinato di: fornire una base giuridica valida per il trattamento e la diffusione delle preferenze degli utenti sotto forma di TC String e di un *cookie euconsent-v2*, vietando al contempo il ricorso a interessi legittimi; assicurare misure di controllo tecniche e organizzative efficaci per garantire l'integrità e la riservatezza della TC String, in conformità con gli artt. 5.1., lett. *f*), 24, 25 e 32 GDPR; mantenere un audit rigoroso delle organizzazioni partecipanti al TCF; adottare

misure tecniche e organizzative per evitare che il consenso sia prestato di default nelle interfacce delle CMP e per impedire l'autorizzazione automatica dei fornitori partecipanti che fondano su interessi legittimi i loro trattamenti, in conformità con gli artt. 24 e 25 GDPR; costringere le CMP ad adottare un approccio uniforme e conforme al GDPR per le informative prestata agli utenti, in conformità con gli artt. 12, 13, 14 e 24 GDPR; aggiornare i registri dei trattamenti, includendo il trattamento dei dati personali nel TCF da parte di IAB Europe, in conformità con l'art. 30 GDPR; effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) sui trattamenti operati nell'ambito del TCF e sul loro impatto sulle attività effettuate nel sistema OpenRTB, con i dovuti riesami in caso di versioni future o modifiche al TCF, conformemente all'articolo del 35 GDPR; nominare un responsabile della protezione dei dati (DPO) in conformità agli artt. 37-39 GDPR. Per il completamento di tali misure è assegnato a IAB Europe un termine massimo di sei mesi dalla convalida di un piano d'azione da parte dell'Autorità, assistito da una penalità di € 5000 per ogni giorno di mancato adempimento. Infine, è comminata a IAB Europe una sanzione amministrativa di € 250.000 ai sensi dell'art. 83, paragrafo 5 GDPR.

VALENTINO RAVAGNANI

<https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf>

2022/1(12)FG

### **La sentenza della Cassazione n. 3952 del 8 febbraio 2022 sul diritto all'oblio e le copie cache**

Con la sentenza n. 3952/2022 dell'8 febbraio 2022, la Corte di Cassazione ha accolto parzialmente il ricorso proposto dalle società Yahoo! EMEA Ltd. e Yahoo! Italia S.r.l. in liquidazione (di seguito collettivamente “**Yahoo!**”) avverso la sentenza del Tribunale di Milano n. 12623/2016, precisando che la richiesta di cancellazione delle copie *cache* relative alle informazioni accessibili tramite un motore di ricerca non può semplicemente accogliersi ogni qual volta sia stato stabilito il diritto alla deindicizzazione, bensì richiede una specifica ponderazione di bilanciamento tra il diritto all'oblio dell'interessato e il diritto del pubblico alla diffusione e alla acquisizione di informazioni relative ai fatti nel loro complesso, attraverso parole chiave anche diverse dal nome della persona.

Nel caso di specie, l'interessato aveva inoltrato al motore di ricerca Yahoo! una richiesta di rimozione dai risultati delle ricerche in Europa di diversi e specifici URL che collegavano il suo nome ad una vicenda giudiziaria da egli ritenuta non più rilevante per il diritto di cronaca (cd. deindicizzazione).

Yahoo! aveva dichiarato di non poter dare riscontro a tale richiesta, ritenendo di non essere qualificabile come titolare di tale trattamento di dati personali. Pertanto, l'interessato aveva depositato un ricorso presso il Garante per la Protezione dei Dati Personali (il “**Garante**”), con le richieste di rimozione degli URL nonché di cancellazione delle copie *cache* dalle pagine web accessibili tramite predetti URL.

Con provvedimento del 25 febbraio 2016, il Garante accoglieva parzialmente le richieste dell'interessato, ingiungendo a Yahoo! di rimuovere gli URL e di cancellare le copie *cache*, pronunciando invece non luogo a provvedere con riferimento ad altre richieste non più rilevanti.

Yahoo! domandava quindi al Tribunale di Milano l'annullamento del provvedimento del Garante. Il Tribunale di Milano confermava il contenuto del provvedimento impugnato e respingeva il ricorso, in quanto riteneva - in primo luogo, in merito alla rimozione degli URL - che sia l'interesse economico delle società e sia l'interesse della collettività a conoscere le informazioni derivanti dalla ricerca riferita al nome dell'interessato, siano in subordine rispetto ai diritti fondamentali dell'interessato stesso e - in secondo luogo, in merito alla cancellazione delle copie *cache* - che il provvedimento del Garante della Privacy fosse in linea con i principi ispiratori del GDPR (Regolamento UE 2016/679), pur pacificamente non applicabile al caso *ratione temporis*, in particolare quanto alla previsione del diritto ad una cancellazione estesa dei dati personali oggetto del trattamento.

Yahoo! impugnava (per cinque motivi) la decisione del giudice di merito dinanzi alla Corte di Cassazione.

La Corte ha rigettato i primi quattro motivi di ricorso confermando la competenza del Garante di emettere i provvedimenti nei confronti di Yahoo!, ai sensi dell'Articolo 7 del d.lgs. 196/2003, l'applicabilità del diritto italiano al caso di specie perché Yahoo! svolge un'attività effettiva e reale nel territorio italiano (sul punto, cfr. anche Corte di Giustizia dell'UE (Terza Sezione), Weltimmo s.r.o. contro Nemzeti Adatvédelmi és Információszabadság Hatóság, causa C-230/14, sentenza del 1° ottobre 2015, par. 41), e la legittimazione passiva della stessa Yahoo!.

Con il quinto motivo di ricorso, la ricorrente criticava, fra l'altro, un'interpretazione del diritto all'oblio sbilanciata in favore dell'interessato (in particolare, "la cancellazione delle copie *cache* delle pagine web accessibili attraverso gli URL"), a detrimento di interessi diversi, come l'interesse dei terzi di accedere alle pagine web per finalità diverse da quelle di una verifica sulle vicende giudiziarie dell'interessato.

Gli ermellini hanno preso in esame sia la rimozione degli URL sia l'eliminazione delle copie *cache*, richiamando i propri precedenti sulle tre nozioni del diritto all'oblio, del diritto alla cancellazione dei dati personali e del diritto alla deindicizzazione.

In particolare, nella sentenza in commento, si ricorda come le Sezioni Unite hanno ricondotto la deindicizzazione nell'ambito del diritto alla cancellazione dei dati, nel quadro della classificazione che considera lo stesso come una delle tre possibili declinazioni del diritto all'oblio, mentre le altre due, sono da individuare nel diritto a non vedere pubblicate nuovamente delle notizie relative a vicende legittimamente diffuse in passato, qualora sia trascorso un congruo periodo di tempo tra la prima e la seconda pubblicazione; ed infine, come esigenza a collocare la pubblicazione, legittimamente avvenuta molto tempo prima, nel contesto attuale (si veda Cassazione, Sezioni Unite, 22 luglio 2019, n. 19681).

La deindicizzazione è strumentale alla tutela giuridica dell'identità digitale dell'interessato e può essere un rimedio per impedire che i dati dell'interessato siano associati dal motore di ricerca ai fatti conservati in rete, venendo incontro al diritto delle persone a non essere trovati facilmente sulla rete.

Nel caso di specie, come già anticipato, la questione specifica affrontata dalla Corte di Cassazione non consisteva nella valutazione di legittimità o meno della deindicizzazione (ossia nel riconoscimento del "*right not to be found easily*"), bensì sulla parte della sentenza impugnata in cui il giudice di merito meneghino ha ritenuto corretto il provvedimento del Garante anche in merito alla cancellazione delle copie *cache* delle pagine web accessibili attraverso gli URL.

Sul punto, la Corte, dopo aver richiamato i principali risultati dell'elaborazione teorica sul diritto all'oblio, i punti 8 e 9 delle Linee guida 5/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca, ai sensi del GDPR adottate il 7 luglio 2020 dal Comitato Europeo per la Protezione dei Dati (<https://edpb.europa.eu/our-work-tools/our->

documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines\_it) e le importanti sentenze del medesimo giudice di legittimità Cass. n. 7559/2020 e Cass. 9147/2020, ha precisato che la cancellazione delle copie *cache*:

1. impedirebbe al motore di ricerca, nell'immediato, di utilizzare le stesse per indicizzare i contenuti per mezzo di parole chiave anche diverse da quella del nome dell'interessato;

2. farebbe sì che il motore di ricerca non potrebbe utilizzare nuove copie *cache* equivalenti a quelle oggetto del provvedimento del Garante che verrebbe, di conseguenza, ad assumere il contenuto di ingiunzione dinamica estendendosi a tutte le copie - con contenuto simile a quelle cui si riferisce il provvedimento - che il motore di ricerca possa realizzare nel futuro.

La valutazione che fa la Corte di Cassazione è che risulta necessario valutare non soltanto il diritto dell'interessato a dissociare l'informazione dal motore di ricerca attraverso l'interrogazione con il suo nome, ma anche l'interesse della collettività a poter trovare quella informazione tramite altri criteri di ricerca, in particolare per mezzo di parole chiave diverse dal nome della persona interessata.

Secondo gli ermellini, la cancellazione delle copie *cache* delle pagine accessibili dalle URL deve tenere conto di una specifica indagine circa il bilanciamento tra l'interesse del singolo ad essere dimenticato e l'interesse della collettività ad essere informata: il giudice di merito ha preso in considerazione solamente l'ambito dell'interessato, relativamente alla concessa indicizzazione, non valutando in maniera adeguata e specifica, quanto alla richiesta della cancellazione delle copie *cache*, l'interesse da parte della collettività ad essere informata sui fatti di cronaca nel suo complesso.

In conclusione, e su questa base, la Corte di Cassazione ha enunciato il seguente principio, rinviando al Tribunale di Milano, in diversa composizione, per farne applicazione: “la cancellazione delle copie *cache* relative a una informazione accessibile attraverso il motore di ricerca, in quanto incidente sulla capacità, da parte del detto motore di ricerca, di fornire una risposta all'interrogazione posta dall'utente attraverso una o più parole chiave, non consegue alla constatazione della sussistenza delle condizioni per la deindicizzazione del dato a partire dal nome della persona, ma esige una ponderazione del diritto all'oblio dell'interessato col diritto avente ad oggetto la diffusione e l'acquisizione dell'informazione, relativa al fatto nel suo complesso, attraverso parole chiave anche diverse dal nome della persona”.

FRANCESCO GROSSI

<https://web.uniroma1.it/deap/sites/default/files/allegati/Cass.-Civ.-Sez.-I-8-febbraio-2022-n.-3952.pdf>

2022/1(13)FDA

### **Le “Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration” dello European Law Institute (ELI) del 3 marzo 2022**

Il 3 marzo 2022 lo *European Law Institute* di Vienna (in breve ELI) ha pubblicato un corposo documento che contiene regole generali sul procedimento diretto a valutare l'impatto («*Impact Assessment*») dei sistemi decisionali basati su algoritmi nella pubblica amministrazione.

Si tratta di un documento programmatico (e non vincolante), adottato sull'esempio di altre proposte redazionali elaborate da altri enti non istituzionali europei (si pensi alle *Model Rules*

on *EU Administrative Procedure* del *Research Network on EU Administrative Law – ReNEUAL*), allo scopo di supportare future legislazioni dell'Unione, dei suoi Stati membri o di altri paesi extracomunitari (così espressamente a p. 12 del documento: «*the Model Rules are intended to be more general and adaptable in different legal contexts within and beyond the EU*») che intendano normare l'uso di sistemi decisionali algoritmici nel settore pubblico (art. 1, par. 1).

Secondo il documento dell'ELI, le decisioni amministrative algoritmiche si possono suddividere in due distinte tipologie: quelle “piene” in cui il processo formativo della volontà pubblica è completamente automatizzato; e quella “semipiene” in cui vi è spazio per la partecipazione umana nel procedimento amministrativo informatico (art. 2, par. 1).

La metodologia operativa suggerita dal documento per soppesare adeguatamente la possibilità di usare algoritmi decisionali nel settore pubblico (al posto o in parziale sostituzione dell'intervento umano) è, come detto, la valutazione d'impatto; la quale, nelle intenzioni dell'ELI, dovrebbe assicurare a ogni amministrazione interessata (e quindi alla cittadinanza) la sicurezza, la completezza, la trasparenza, l'accessibilità e la responsabilità della soluzione organizzativa prescelta.

Scendendo nel dettaglio, il documento dell'ELI è composto da cinque capitoli suddivisi in sedici articoli e quattro allegati.

Esso parte dal presupposto che l'uso di sistemi algoritmici nella pubblica amministrazione non può seguire un unico approccio operativo («*precludes a one-size fits all approach*»); così si legge a p. 11), ma va opportunamente calibrato al contesto e all'ente di riferimento (la «*Implementing Authority*») secondo la dizione dell'art. 2, par. 2, n. 7).

Distingue perciò tra sistemi ad “alto rischio” (ossia a più elevato impatto sociale come l'ambiente, le telecomunicazioni, il fisco, le infrastrutture) per i quali è sempre consigliata una valutazione d'impatto rafforzata (allegato 1); sistemi a “basso rischio” (dove le criticità sono ben note e facilmente gestibili per legge) che ne sono esentati (allegato 2); sistemi a “medio rischio” per cui è richiesta una verifica d'impatto semplificata (art. 4); sistemi “incerti” e soggetti, in quanto tali, a una verifica preliminare per accertare in quale delle tre categorie principali rientrano (allegato 3).

In caso di valutazione d'impatto semplice (e sempre che non ricorrano particolari motivi di celerità o emergenza menzionati espressamente all'art. 1, par. 4 del documento dell'ELI) la procedura da seguire prevede la redazione di un piano d'azione (art. 6), anche col supporto di enti specializzati (art. 5), che deve contenere chiare ed esaustive informazioni: a) sul tipo di algoritmo che l'amministrazione procedente intenderà usare, sulle sue caratteristiche tecniche, sul suo modo di funzionamento, sulle finalità che esso vuole conseguire; b) sulla tutela dei diritti dei privati, sulle ricadute sociali, sui benefici della scelta organizzativa dell'amministrazione procedente; c) sulla sicurezza, tracciabilità, legalità e proporzionalità delle future decisioni prese dall'algoritmo; d) sulle garanzie tecniche fornite dal produttore del sistema informatico acquistato dall'amministrazione (art. 7); e) sulla protezione dei dati personali e della proprietà intellettuale (art. 8). Il documento così elaborato dev'essere pubblicato telematicamente dalla autorità procedente per raggiungere la più ampia platea di destinatari (art. 13).

Se invece è richiesta la valutazione d'impatto rafforzata, tra la pubblicazione del piano di azione e la sua diffusione al pubblico, si insinua una fase istruttoria che prevede: a) la consultazione di un collegio tecnico indipendente (i cui membri sono selezionati con criteri obiettivi dall'amministrazione procedente) chiamato a verificare la adeguatezza e la precisione del piano d'azione (art. 10); l'avvio di un dibattito pubblico per permettere ai destinatari dell'azione amministrativa di partecipare al procedimento di valutazione d'impatto (art. 11, par. 1: «*ensure that those specifically affected by the system are afforded the opportunity to participate in this*

*process*). Al termine del percorso appena descritto l'autorità procedente pubblica in via definitiva il piano d'azione motivato sulla base dei dati istruttori raccolti (art. 12).

Da ultimo, il documento dell'ELI si preoccupa di indicare gli strumenti di tutela rispetto alla valutazione d'impatto.

Anzitutto sottolinea che l'autorità procedente possa sempre aggiornare o ripetere la valutazione in caso di errori inattesi o di sopravvenute necessità anche di ordine istruttorio (se emerge, cioè, «*substantial negative impact*» o «*additional knowledge gained during the practical use of the system*»: art. 14, par. 1 e par. 2, lett. b); in secondo luogo suggerisce di sottoporre ogni valutazione d'impatto al controllo esterno di un'autorità amministrativa indipendente (individuata esplicitamente nell'Autorità nazionale garante dei dati personali: si veda la p. 50 del documento dell'ELI) con poteri d'inchiesta, proposta e sanzionatori (art. 15), i cui provvedimenti devono sottostare in ogni caso al vaglio giurisdizionale (art. 16, par. 3).

FILIPPO D'ANGELO

[https://www.europeanlawinstitute.eu/news-events/news-contd/news/eli-issues-guidance-on-the-use-of-algorithmic-decision-making-systems-by-public-administration/?tx\\_news\\_pi1%5Bcontroller%5D=News&tx\\_news\\_pi1%5Baction%5D=detail&cHash=f4a2a4a677e3dcf6e391d9f0a2a9bd6a](https://www.europeanlawinstitute.eu/news-events/news-contd/news/eli-issues-guidance-on-the-use-of-algorithmic-decision-making-systems-by-public-administration/?tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=f4a2a4a677e3dcf6e391d9f0a2a9bd6a)

2022/2(1)RA

### **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 [2021/4\(4\)RA](#)), 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 [2022/1\(2\)RA](#) e [2022/1\(4\)SO](#)), 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) DGA).

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>

**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 si 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 Resilience Act: “DORA*”) e sui *Markets in Crypto-Assets (“Regolamento MiCA*”: su cui vedi la notizia successiva [2022/2\(3\)AF](#)), 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, architetture decentralizzate 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”, ovvero sia 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 essere disciplinato dal Regolamento MiCA (sul quale v. più in particolare la notizia successiva [2022/2\(3\)AF](#)). 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.

Innanzitutto, 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>

2022/2(3)AF

### **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 [2020/4\(2\)MS](#)).

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/>

2022/2(4)FG

**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 [2022/1\(1\)EB](#)).

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 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 contengono 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>

2022/2(5)SO

**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 [2022/1\(1\)EB](#)); 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 riservano 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'LA 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 LA. (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'LA [...]”.

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>

2022/2(6)EMI

**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 *Absolut's -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>

2022/2(7)VR

**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 *in vi* 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 necessità. 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 allorché 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 espliciti 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 antitetico 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, viepiù 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](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](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 [2021/3\(3\)CR](https://www.congiunti.it/2021/3(3)CR)). 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](https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_it)

## **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 [2021/2\(1\)SO](#)). 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).

Senonché, 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 *“evinca 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 LA che collegano vendite, transazioni e dati sulle prestazioni ... Analogamente, i sistemi di LA 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>

2022/2(9)ES

### **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>

2022/2(10)AAM

### **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 cerebrale (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 Stanzone, 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. Stanzone 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 inespresi 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 cerebrali, 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 neurotecnologie 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 informativo 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>

2022/2(11)AF

### **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 *national 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 in 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](https://www.banking.senate.gov/imo/media/doc/the_stablecoin_trust_act.pdf)

2022/2(12)VP

### **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 PITELLI

2022/3(1)TDMCDV

## **Verso la AI Liability Directive: la proposta della Commissione europea del 28 settembre 2022 per una direttiva sull'adattamento delle regole di responsabilità civile all'Intelligenza Artificiale.**

Il 28 settembre 2022 la Commissione europea ha pubblicato due proposte di direttiva che si collocano all'interno di un "pacchetto" di misure atte a sostenere gli obiettivi di "eccellenza e fiducia" relativi all'Intelligenza Artificiale (IA) come già delineati nei precedenti documenti istituzionali dell'Unione. In particolare, tale pacchetto – come si evince dalla relazione di accompagnamento (*Explanatory Memorandum*) – comprende tre linee di intervento tra loro complementari: 1) la proposta di regolamento del 21 aprile 2021 su regole armonizzate e orizzontali sull'Intelligenza Artificiale (*AI Act*) su cui v. la notizia [2021/2\(1\)SO](#) una revisione di norme in tema di sicurezza dei prodotti, tanto settoriali quanto orizzontali; 3) l'armonizzazione di regole di responsabilità civile adeguate alle caratteristiche dei moderni sistemi di Intelligenza Artificiale.

All'interno del terzo filone di interventi citati, la prima proposta stabilisce l'armonizzazione di alcuni profili probatori inerenti ai regimi di responsabilità civile esistenti negli Stati membri e fondati sul criterio della colpa, in modo da garantire che i soggetti danneggiati da un sistema di IA cd. "ad alto rischio" godano di un livello di protezione equivalente a quello di cui godrebbero se i danni in questione fossero stati causati senza il coinvolgimento di un sistema di IA (Considerando n. 7). A tal fine, si prevedono in favore del danneggiato meccanismi di semplificazione probatoria potenzialmente in grado di supplire alle difficoltà generate dalle peculiarità dei sistemi di IA, caratterizzati da funzioni di c.d. auto-apprendimento, nonché da scarsa comprensibilità (opacità) da parte del soggetto danneggiato chiamato a provare in giudizio la condotta colposa del responsabile e il nesso di causalità tra questa e il danno.

La proposta in esame fa seguito, specificamente, alla Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL), già illustrata su questa Rubrica alla notizia [2020/4\(1\)SG](#).

Essa, tuttavia, condivide poco o niente con la proposta del Parlamento europeo. *In primis*, differente è la scelta dello strumento normativo: il regolamento nella Risoluzione, la direttiva nella proposta della Commissione. In secondo luogo, la *AI Liability Directive* propone una forma di armonizzazione dei regimi di responsabilità civile esistenti tra gli Stati membri, mentre la Risoluzione del 2020 elaborava nuove forme di responsabilità *ad hoc* – seppure non limitative di altri regimi di responsabilità esistenti – in capo agli operatori di sistemi di IA, introducendo le nozioni di operatore di *back-end* e di *front-end*. Da ultimo, mentre la proposta di Regolamento prevedeva un regime di responsabilità oggettiva di detti operatori (fondata sul rischio e sul grado di controllo su di esso esercitato da ciascuno), la Commissione ha optato per armonizzare unicamente i regimi di responsabilità per colpa esistenti a livello nazionale, demandando alla futura revisione della direttiva la valutazione intorno all'opportunità di introdurre regimi di responsabilità oggettiva, così come forme di assicurazione obbligatoria.

L'iniziativa, dunque, si propone di completare il quadro di tutele approntate dall'*AI Act*, che prevede l'imposizione di taluni obblighi gravanti *ex ante* su fornitori e utenti di sistemi di

IA “ad alto rischio” nella fase di immissione del software sul mercato. La proposta, in questo modo, intende contribuire all’effettività dei suddetti requisiti, poiché la non conformità del sistema di IA agli standard previsti dall’*AI Act* è in grado di attivare *ex post* i meccanismi di alleggerimento probatorio proposti dalla Commissione in caso di verifica di eventi dannosi causalmente riconducibili al sistema stesso. Il testo si compone di 9 articoli, di cui si espongono di seguito i tratti salienti.

L’art. 1 circo-scrive oggetto e scopo della direttiva. Essa stabilisce regole armonizzate in tema di “*disclosure*” di prove per i sistemi di IA ad alto rischio e di onere della prova nei casi di richieste di risarcimento danni proposte davanti ai giudici nazionali a titolo di responsabilità extracontrattuale e fondate sul criterio di imputazione della colpa. Allo stesso tempo, precisa la Commissione, la direttiva non incide: sulle norme del diritto dell’Unione che disciplinano le condizioni di responsabilità nel settore dei trasporti; sui diritti da chiunque azionabili in virtù delle norme nazionali di recepimento della Direttiva 85/374/CEE (cd. “responsabilità del produttore”); sulle norme nazionali che determinano a chi spetta l’onere della prova, il grado di certezza richiesto in ordine alla stessa, ovvero il modo in cui viene definita la colpa, al di fuori di quanto previsto dagli articoli 3 e 4. Inoltre, agli Stati membri è consentito adottare o mantenere norme nazionali più favorevoli per i danneggiati, purché compatibili con il diritto dell’Unione, dunque anche regimi di responsabilità oggettiva esistenti a livello nazionale e fondati su elementi diversi dal difetto del prodotto (Considerando n. 11).

Dalle definizioni di cui all’art. 2 emerge con tutta evidenza la finalità di coordinamento tra la proposta in esame e la proposta di *AI Act*, il cui contenuto viene richiamato *per relationem* con riguardo alle nozioni di “sistema di IA”, “sistema di IA ad alto rischio”, “fornitore” e “utente”. In aggiunta, viene precisato il significato di alcune locuzioni, tra cui spicca quella di “richiesta di risarcimento” (*claim for damages*), che viene circoscritta al danno causato da un *output* prodotto da un sistema di IA o dall’omissione di tale sistema nel produrre un *output* laddove esso avrebbe dovuto essere prodotto.

Nucleo centrale della proposta sono i sistemi di semplificazione probatoria di cui agli artt. 3 e 4 in favore del danneggiato. All’art. 3 si prevede un meccanismo di cd. “*disclosure*” probatoria, cui consegue eventualmente una presunzione di colpa del fornitore (o di un soggetto a questo equiparato) ovvero dell’utente del sistema di IA. Il giudice nazionale ha il potere di ordinare a tali soggetti di produrre prove relative a specifici sistemi di IA ad alto rischio sospettati di aver causato un danno, purché la relativa richiesta sia proporzionata. La proposta di direttiva non specifica in cosa debbano consistere tali prove, ma prevede che per stabilire se una richiesta di prove sia proporzionata il giudice deve prendere in considerazione i segreti commerciali nel significato di cui all’articolo 2(1) della Direttiva (EU) 2016/943 e le informazioni confidenziali quali le informazioni relative alla sicurezza pubblica o nazionale.. Tale potere è esercitabile dal giudice in un duplice momento: sia in via anticipatoria, qualora cioè venga proposta istanza da un attore “potenziale” (*potential claimant*, ossia che non ha ancora proposto domanda giudiziale), il quale abbia previamente richiesto tale esibizione ai suddetti soggetti senza ottenere riscontro, purché fornisca elementi sufficienti a sostenere la plausibilità della domanda risarcitoria; sia su richiesta dell’attore nel corso di un giudizio già avviato. In questo modo si consente all’attore di ottenere informazioni che devono essere conservate a norma dell’*AI Act*, il quale tuttavia non prevede il corrispondente diritto del danneggiato di accedervi (Considerando 16). Il giudice può anche ordinare la conservazione della prova nei modi che ritenga più consoni.

Qualora il convenuto non ottemperi all’ordine di esibizione o conservazione della prova, scatta la presunzione di inosservanza da parte del convenuto dei doveri di attenzione (*duty of care*) relativi al sistema di IA per cui era stato pronunciato l’ordine, rilevanti a livello nazionale

ed europeo, con particolare riferimento ai requisiti posti dall'*AI Act*. La presunzione in esame ha carattere relativo, in quanto è superabile dal convenuto a norma dell'ultimo paragrafo dell'art. 3 fornendo prova contraria (Considerando n. 21, art. 3 par. 5). L'art. 3 delinea, dunque, un regime di responsabilità per colpa di fornitori e utenti per la mancata ottemperanza agli standard posti dall'*AI Act*, la cui prova gravante sul danneggiato viene alleggerita tramite un meccanismo di *disclosure* a carico del convenuto e una eventuale presunzione di colpa del convenuto, che interviene nel caso di sua mancata ottemperanza all'ordine di *disclosure*. Esso contempla solo quei danni che siano la manifestazione di un rischio specificamente contemplato dalla normativa di sicurezza *ex ante* (Considerando 22 e 25).

Il secondo strumento presuntivo, fissato dall'art. 4, concerne il nesso di causalità tra la condotta colposa del convenuto e l'*output* prodotto dal sistema di IA, oppure, secondo il caso, tra la condotta colposa del convenuto e la mancata produzione da parte del sistema di IA dell'*output* che il sistema di IA avrebbe dovuto produrre. Tale presunzione opera, ed è rilevante, subordinatamente all'avverarsi di tutte le seguenti condizioni: a) l'attore ha provato – o il giudice ha presunto ex art. 3 – la colpa del convenuto, consistente nella violazione di un dovere di attenzione (*duty of care*) rilevanti a livello nazionale ed europeo, diretti a prevenire la tipologia di danno occorso; b) si può ritenere ragionevolmente probabile, in base alle circostanze del caso, che la colpa del convenuto abbia influenzato l'*output* generato dal sistema, ovvero la sua mancata produzione; c) l'attore ha provato il nesso di causalità tra il danno subito e l'*output* o la sua mancata produzione da parte del sistema di IA. Il par. 2 dell'art. 4 specifica che la condizione di cui alla lett. a) dovrebbe ritenersi integrata unicamente qualora l'attore abbia dimostrato che il fornitore o l'utente non si sono conformati ai requisiti stabiliti dai capi 2 e 3 del Titolo III dell'*AI Act*. In particolare, si fa riferimento alla inosservanza degli obblighi: a) di cui all'art. 10, parr. 2-4 dell'*AI Act*, in caso di mancato sviluppo del sistema tramite fasi di addestramento, convalida e test di set di dati che soddisfano i criteri di qualità ivi contenuti; b) di trasparenza (art. 13 *AI Act*); c) di supervisione umana (art. 14 *AI Act*); d) di accuratezza, robustezza e cybersicurezza (artt. 15 e 16 *AI Act*). La norma considera, poi, specificamente i profili di colpa dell'utente, facendo riferimento alla violazione degli obblighi previsti dall'art. 29 dell'*AI Act* (obbligo di utilizzare il sistema secondo le istruzioni per l'uso, obbligo di interrompere l'uso quando necessario, qualora abbia esposto il sistema a *input* rientranti nel suo controllo) e precisando che, qualora si tratti di utente non professionale, la presunzione opera solo se dimostrato che questo abbia concretamente interferito con il funzionamento del sistema. Anche la presunzione di causalità di cui all'art. 4 è superabile dal convenuto, dimostrando, ad esempio, che la sua condotta non può aver cagionato il danno (Considerando n. 30, art. 4 par. 7). Inoltre, la presunzione è preclusa *ab origine* all'attore qualora il convenuto dimostri che la prova di cui è stata ordinata la *disclosure* era facilmente accessibile al danneggiato. Occorre rilevare, infine, che la medesima norma contempla l'ipotesi di danni cagionati da sistemi di IA non ad alto rischio (i quali non sono soggetti ai requisiti obbligatori dell'*AI Act*), prevedendo che la presunzione di causalità debba applicarsi tutte le volte in cui il giudice ritenga eccessivamente complesso per il danneggiato fornire la relativa prova.

Ai sensi dell'art. 5, la Direttiva sarà sottoposta a revisione dopo cinque anni dalla sua entrata in vigore al fine di valutare l'eventuale opportunità di introdurre forme di responsabilità oggettiva e di assicurazione obbligatoria.

TOMMASO DE MARI CASARETO DAL VERME

[https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence\\_en](https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en)

2022/3(2)TDMCDV

**Verso la nuova Product Liability Directive: la proposta della Commissione europea del 28 settembre 2022 per una nuova direttiva sulla responsabilità da prodotto difettoso che abroga la Direttiva 85/374/CEE.**

La seconda proposta della Commissione in tema di responsabilità civile consiste in una nuova direttiva sulla responsabilità da prodotto difettoso, in sostituzione della Direttiva 85/374/CEE (*Product Liability Directive*: PLD). Essa risponde alla necessità, avvertita dalle istituzioni eurounitarie, di rivedere la vigente PLD alla luce delle moderne evoluzioni della tecnologia, con particolare riguardo ai sistemi di IA. Tali istanze sono emerse, da ultimo, tanto nella citata Risoluzione del Parlamento europeo del 20 ottobre 2020 (su cui v. su questa Rubrica la notizia [2020/4\(1\)SG](#)), quanto nella successiva valutazione di impatto (*Inception Impact Assessment*) della Commissione del 30 giugno 2021 intitolata “*Adapting liability rules to the digital age and circular economy*” ([https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en)).

In particolare, il Parlamento, pur rilevando la generale adeguatezza della direttiva ad affrontare i danni cagionati da *smart products*, sottolineava in quella risoluzione la necessità di adeguare alcune nozioni in essa contenute – tra cui “prodotto”, “difetto” e “produttore” – alla più recente evoluzione tecnologica, nonché di considerare l'inversione dell'onere della prova per i danni causati dalle tecnologie digitali emergenti in casi chiaramente definiti e previa un'adeguata valutazione. La Commissione, a sua volta, nella citata valutazione di impatto, suggeriva di estendere il regime di responsabilità oggettiva in questione anche ai prodotti immateriali (ad es. contenuti digitali e software), nonché ai difetti risultanti da modifiche subite dai prodotti dopo la loro immissione sul mercato (ad es. aggiornamenti del software), ai difetti risultanti da interazioni con altri prodotti e servizi (ad es. IoT) ed ai rischi ricollegati alla connettività ed alla cybersicurezza. Inoltre, la Commissione proponeva di alleggerire l'onere della prova gravante sul consumatore-danneggiato, invertendo l'onere della prova e precludendo al convenuto la prova liberatoria del cd. “rischio da sviluppo” nei casi di danni cagionati da sistemi di IA con funzioni di c.d. auto-apprendimento e adattamento.

La proposta in esame intende completare la tutela approntata dalla *AI Liability Directive* (su cui v. la notizia precedente [2022/3\(1\)TDMCDV](#)), la quale, se introduce un regime “semplificato” di responsabilità degli operatori di sistemi di IA ad alto rischio, considera tuttavia solo i regimi di responsabilità extracontrattuale per colpa e, peraltro, non contempla tutti i rischi derivanti dalla produzione e dall'utilizzo di *smart products*, ma solo quelli ricollegati ai requisiti posti dalla normativa di sicurezza *ex ante*. Il sistema della responsabilità da prodotto difettoso, invece, attribuisce al danneggiato una forma di tutela più ampia, in quanto prescinde dalla colpa del produttore e consente di considerare difettoso anche un prodotto conforme alle norme di sicurezza. La complessità che caratterizza le moderne tecnologie (non solo di IA, ma anche i nuovi modelli di business dell'economia circolare e le nuove *supply chain* globali) pone, tuttavia, i suddetti interrogativi circa la perdurante efficienza e operatività della vigente PLD, cui la proposta della Commissione tenta di fornire una prima risposta. La proposta si compone di venti articoli suddivisi in quattro capi. Di seguito si espongono le principali novità rispetto alla normativa vigente.

L'art. 4 fornisce una vasta gamma di definizioni che vogliono rispecchiare l'evoluzione tecnologica in ambito digitale. In particolare, alla definizione di «prodotto» di cui all'art. 2 della vigente PLD si aggiungono i *file* di produzione digitale (“*digital manufacturing file*”, ossia una versione digitale o un modello digitale di un bene mobile) e i *software*. Similmente, la nozione di «componente» include qualsiasi bene, materiale o immateriale, o qualsiasi servizio correlato, integrato o interconnesso con un prodotto. Il novero dei danni risarcibili viene ampliato, comprendendo, oltre alla morte, alle lesioni personali e ai danni a cose diverse dal prodotto stesso (art. 9 della proposta di nuova PLD): i danni alla salute psicologica medicalmente accertabili; il danneggiamento o la distruzione di qualsiasi bene, eccetto un prodotto danneggiato da una componente difettosa dello stesso e beni utilizzati per scopi professionali; la perdita o il danneggiamento di dati non utilizzati esclusivamente a fini professionali.

La definizione di «prodotto difettoso» di cui all'art. 6 della vigente PLD viene arricchita e maggiormente specificata dall'art. 6 della proposta. Un prodotto è difettoso quando non offre la sicurezza che la generalità dei consociati o il “grande pubblico” (“*public at large*”) può legittimamente attendersi. Nel memorandum di accompagnamento della proposta, si trova scritto che il relativo test è sostanzialmente lo stesso di quello richiesto dalla vigente PLD, ma che, per tener conto della natura dei prodotti nell'era digitale e per riflettere la giurisprudenza della Corte di Giustizia dell'Unione Europea, alcuni fattori sono stati aggiunti alla lista non esaustiva dei fattori di cui i giudici devono tener conto nell'accertare la difettosità, tra cui l'interconnessione e le funzioni di auto-apprendimento. In particolare, le circostanze di cui tenere conto, tra le altre, ai fini della valutazione intorno alla difettosità del prodotto ora includono: a) nella presentazione del prodotto, le istruzioni per l'installazione, l'uso e la conservazione del prodotto; b) l'uso corretto o distorto ragionevolmente prevedibile; c) gli effetti sul prodotto causati dalla sua abilità di apprendere successivamente al rilascio sul mercato; d) gli effetti causati sul prodotto da altri prodotti con cui esso entra in contatto; e) oltre al momento della messa in circolazione del prodotto, anche quello in cui il produttore perde il controllo sullo stesso qualora questo perduri anche successivamente al rilascio; f) i requisiti di sicurezza del prodotto, compresi quelli di cybersicurezza; g) qualsiasi intervento di un'autorità di regolazione o di un operatore economico di cui all'articolo 7 relativo alla sicurezza dei prodotti; h) le aspettative dello specifico utente finale cui il prodotto è destinato. Infine, la regola per cui la sola esistenza di un prodotto più evoluto non può rendere il prodotto difettoso include ora anche gli aggiornamenti dello stesso.

Maggiormente dettagliata è la nozione di «produttore» fornita dall'art. 7 della proposta di nuova PLD, con cui la Commissione si preoccupa, in particolare, di specificare la responsabilità solidale del produttore della singola componente difettosa, così come la responsabilità dell'importatore nel caso in cui il produttore sia stabilito al di fuori dell'Unione.

All'art. 8 della proposta di nuova PLD è previsto un meccanismo di *disclosure* simile a quanto visto nella coeva proposta di *AI Liability Directive* (su cui v. notizia precedente [2022/3\(1\)TDMCDV](#)), impiegabile unicamente nel corso del giudizio e purché l'attore abbia fornito elementi sufficienti a fondare la plausibilità della propria domanda risarcitoria. La mancata ottemperanza all'ordine attiva, anche in questo caso, una presunzione (relativa) che, però, concerne la prova del difetto. All'art. 9 della proposta di nuova PLD, infatti, l'onere della prova gravante sul danneggiato rimane invariato rispetto alla vigente PLD, tuttavia con l'aggiunta che il prodotto si presume difettoso se, alternativamente: a) il produttore non abbia ottemperato all'ordine di *disclosure*; b) l'attore dimostri che il prodotto non è conforme a standard di sicurezza obbligatori che ricomprendono la stessa tipologia di rischio di cui al danno occorso; ovvero c) l'attore provi un palese malfunzionamento del prodotto durante un impiego normale dello stesso.

La medesima norma stabilisce che si presume anche il nesso di causalità tra difetto e danno, ove sia accertato il difetto del prodotto e la compatibilità tra la natura del danno cagionato e il difetto in questione. In ogni caso, il giudice, qualora constati una eccessiva complessità probatoria gravante sul danneggiato, può presumere il difetto e il nesso di causalità qualora il danneggiato abbia fornito elementi sufficienti a provare che il prodotto ha contribuito alla verificazione del danno e che è probabile che il prodotto fosse difettoso o che la difettosità sia stata causa probabile del danno. Con tale disposizione viene positivizzata un'istanza di tutela avanzata da più parti (soprattutto in dottrina), tesa a valorizzare il fattore della “verosimiglianza” con riguardo alla prova del difetto (e non limitato alla prova liberatoria del “difetto sopravvenuto”).

L'art. 10 della proposta di nuova PLD in tema di esclusione della responsabilità ripercorre quasi pedissequamente quanto previsto dall'art. 7 della vigente PLD, ma articola le prove liberatorie in rapporto alle rinnovate categorie di soggetti responsabili. Particolare rilievo assume la circostanza per cui l'applicazione del “rischio da sviluppo” (lett. f) viene limitata al produttore, precludendo dunque all'importatore e al distributore di avvalersene. Costituisce assoluta novità, invece, quanto previsto dal secondo paragrafo dell'art. 10 della proposta di nuova PLD, che esclude l'esenzione da responsabilità per il cd. “difetto sopravvenuto” previsto dalla lettera c) del par. 1 del medesimo articolo, qualora il difetto, in costanza di possibilità di controllo da parte del fabbricante, sia causato da: a) un servizio correlato; b) il software, inclusi i suoi aggiornamenti; c) la mancanza di aggiornamenti ove necessari per garantire la sicurezza del prodotto.

Sostanzialmente invariati rimangono i termini di prescrizione e decadenza di cui alla vigente PLD. Degna di nota è, infine, la disposizione dell'art. 3 della proposta di nuova PLD sul livello di armonizzazione della Direttiva, che preclude agli Stati membri di mantenere o introdurre disposizioni divergenti da quelle stabilite nella proposta, comprese disposizioni più o meno rigorose per conseguire un diverso livello di protezione dei consumatori, salvo diversa disposizione della direttiva stessa. Tale previsione, assente nella versione vigente della direttiva, appare tesa a neutralizzare lo spazio di discrezionalità che la vigente PLD aveva concesso agli Stati nel suo recepimento - specialmente con riguardo alla prova del rischio da sviluppo (art. 15, lett. b) della vigente PLD) – e che spesso è stata additata come responsabile di un sostanziale fallimento nell'armonizzazione del livello di tutela dei consumatori danneggiati nel territorio dell'Unione.

TOMMASO DE MARI CASARETO DAL VERME

[https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd\\_en](https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en)

2022/3(3)RA

**Proposta di Regolamento riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (Data Act): First Presidency compromise text del 12 luglio 2022.**

Il 12 luglio 2022, a seguito di un lungo *iter* iniziato lo scorso 23 febbraio 2022 e sulla base dei suggerimenti forniti dagli Stati membri, la Presidenza del Consiglio dell'Unione Europea ha redatto un primo (parziale) *compromise text* della proposta di Regolamento riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (“**Proposta di Data Act**” o

“DA”; v. notizia [2022/1\(4\)SO](#)). Il *compromise text* concerne i soli Capi I, II, III e IV della Proposta di Data Act e i relativi Considerando.

Dalle modifiche effettuate dalla Presidenza del Consiglio al **Capo I** del DA emerge, anzitutto, che essa si occupa di stabilire non solo, come già indicato nella originaria proposta della Commissione, “*norme armonizzate relative alla messa a disposizione dei dati generati dall’uso di un prodotto o di un servizio correlato all’utente di tale prodotto o servizio, alla messa a disposizione di dati da parte dei titolari dei dati ai destinatari dei dati, alla messa a disposizione di dati da parte dei titolari dei dati agli enti pubblici o alle istituzioni, agenzie o organismi dell’Unione, a fronte di necessità eccezionali, per l’esecuzione di un compito svolto nell’interesse pubblico*”, bensì anche quelle relative “*alla facilitazione del passaggio da un servizio di trattamento dei dati all’altro, all’introduzione di garanzie contro l’accesso illegale di terzi ai dati non personali e allo sviluppo di standard di interoperabilità per i dati da trasferire e utilizzare*” (art. 1 (1) DA).

Il nuovo paragrafo (1a) dell’art. 1 chiarisce, ora, che il DA riguarda “*dati personali e non personali, compresi i seguenti tipi di dati o nei seguenti contesti: (a) il Capo II si applica ai dati relativi alle prestazioni, all’uso e all’ambiente dei prodotti e dei servizi correlati; (b) il Capo III si applica a tutti i dati del settore privato soggetti agli obblighi di condivisione dei dati previsti dalla legge; (c) il Capo IV si applica a tutti i dati del settore privato a cui si accede e che vengono utilizzati sulla base di accordi contrattuali tra aziende; (d) il Capo V si applica a tutti i dati del settore privato con particolare attenzione ai dati non personali; (e) il Capo VI si applica a tutti i dati trattati dai servizi di elaborazione dati; (f) il Capo VII si applica a tutti i dati non personali conservati nell’Unione da fornitori di servizi di elaborazione dati*”.

Mediante alcune modifiche all’art. 1(2), il *compromise text* presidenziale meglio illustra l’ambito territoriale di applicazione della Proposta di Data Act, stabilendo che con riguardo ai fabbricanti di prodotti e ai fornitori dei servizi immessi nel mercato dell’Unione, nonché ai titolari dei dati che mettono dati a disposizione dei destinatari dei dati nell’Unione, il DA si applica indipendentemente dal loro luogo di stabilimento. Il principio di irrilevanza del luogo di stabilimento trova ora applicazione anche in relazione ai fornitori di servizi di trattamento dei dati che offrono tali servizi a clienti nell’Unione.

I paragrafi (3), (4) e (4a) dell’art. 1 del DA – a seguito delle recenti modifiche – chiariscono, invece, il rapporto della Proposta di Data Act con la restante disciplina vigente; in particolare, stabiliscono che la proposta in commento non pregiudica l’applicazione del GDPR (e dell’ulteriore disciplina in materia di protezione dei dati personali, della privacy e della riservatezza delle comunicazioni e dell’integrità delle apparecchiature terminali) e del regolamento (UE) 2018/1807 sulla libera circolazione dei dati non personali nell’Unione.

Il *compromise text* presidenziale ha aggiunto, inoltre, alcune definizioni all’art. 2 del DA – tra le quali quella di ‘dato personale’ e ‘dato non personale’, nonché di ‘consenso’ e ‘interessato’ – effettuando un semplice richiamo a quelle fornite dall’art. 4 del GDPR (v. art. 2, nn. 1a, 1ab, 1ac e 1ad DA); altre definizioni di cui al medesimo art. 2 sono state, invece, solamente in parte modificate. Tra queste, rivestono un rilievo cruciale ai fini del regolamento quelle di:

- ‘prodotto’: “*un bene materiale che ottiene, genera o raccoglie dati relativi al suo utilizzo o al suo ambiente e che è in grado di comunicare dati tramite un servizio di comunicazione elettronica accessibile al pubblico e la cui funzione primaria non è la conservazione e il trattamento dei dati né è progettato principalmente per visualizzare o riprodurre contenuti, o per registrare e trasmettere contenuti*” (art. 2, n. 2 DA);
- ‘servizio correlato’: “*un servizio digitale, anche software, che al momento dell’acquisto, dell’affitto o del contratto di noleggio è interconnesso con un prodotto in modo tale che la sua assenza impedirebbe al prodotto di svolgere una delle sue funzioni*” (art. 2, n. 3 DA);

- ‘assistenti virtuali’: “*un software che può elaborare richieste, compiti o domande, incluse quelle basate su input sonori o scritti, gesti o movimenti, e che, sulla base di tali richieste, compiti o domande, fornisce accesso ad altri servizi o controlla dispositivi fisici collegati*” (art. 2, n. 4 DA);
- ‘utente’: “*una persona fisica o giuridica, incluso un interessato, che possiede, affitta o noleggia un prodotto o riceve un servizio correlato*” (art. 2, n. 5 DA);
- ‘titolare dei dati’: “*una persona fisica o giuridica che ha il diritto o l’obbligo, conformemente al presente regolamento, al diritto applicabile dell’Unione o alla legislazione nazionale di attuazione del diritto dell’Unione, o, nel caso di dati non personali e attraverso il controllo della progettazione tecnica del prodotto e dei servizi correlati, la capacità di mettere a disposizione determinati dati*” (art. 2, n. 6 DA).

Il *compromise text* ha poi previsto una modifica alla rubrica del **Capo II** del DA, che ora è intitolato “*Diritto degli utenti di utilizzare i dati dei prodotti connessi e dei servizi correlati*”, al fine di riflettere in modo più preciso gli obiettivi del Capo in parola.

L’art. 3 del DA, all’esito delle modifiche effettuate dalla Presidenza del Consiglio dell’UE, ora dispone – innanzitutto – che i prodotti devono progettati e fabbricati, e i servizi correlati forniti, in modo tale che i dati generati dal loro uso che sono accessibili al titolare dei dati siano, per impostazione predefinita e gratuitamente, facilmente, in maniera sicura e, ove pertinente e opportuno, accessibili all’utente in un formato strutturato, comunemente utilizzato e leggibile a macchina (art. 3(1) DA); in secondo luogo, che prima di concludere un contratto di acquisto, affitto o noleggio di un prodotto o di un servizio correlato, il titolare dei dati deve fornire (almeno) una serie di informazioni indicate all’art. 3(2) del DA.

L’art. 4(1) del DA – così come risultante dalle modifiche del *compromise text* – stabilisce, invece, che qualora l’utente non possa accedere direttamente ai dati a partire dal prodotto o dal servizio correlato, il titolare dei dati deve comunque mettere a disposizione dell’utente i dati generati dall’utilizzo del prodotto o del servizio correlato che sono accessibili al medesimo titolare (oltre ai i metadati rilevanti), senza indebito ritardo, gratuitamente, facilmente, in maniera sicura, in un formato strutturato, comunemente utilizzato e leggibile a macchina e, ove applicabile, in modo continuo e in tempo reale. Ciò dovrà avvenire sulla base di una semplice richiesta mediante mezzi elettronici, ove tecnicamente fattibile.

Ai sensi dell’art. 4(2)-(6) del DA, resta fermo che: 1) il titolare dei dati non può imporre all’utente di fornire informazioni al di là di quanto necessario per verificare la sua qualifica e che il titolare non potrà conservare informazioni relative all’accesso dell’utente ai dati richiesti; 2) come stabilito al nuovo punto 2a, il titolare dei dati non deve costringere, ingannare o manipolare in alcun modo l’utente sovvertendo o compromettendo l’autonomia, il processo decisionale o le scelte di questo al fine di ostacolarne l’esercizio del diritto di accesso; 3) i segreti commerciali sono comunicati solo a condizione che siano adottate in anticipo tutte le misure specifiche necessarie per tutelarne la riservatezza; 4) l’utente non può utilizzare i dati ottenuti per sviluppare un prodotto in concorrenza con quello da cui provengono i dati; 5) come stabilito al nuovo punto 5a, l’utente non deve ricorrere a mezzi coercitivi o abusare di evidenti lacune nell’infrastruttura tecnica del titolare dei dati al fine di ottenere l’accesso ai dati; 6) qualora l’utente non sia l’interessato cui si riferiscono i dati personali richiesti, i dati personali generati dall’uso di un prodotto o di un servizio correlato sono messi a disposizione dell’utente dal titolare dei dati solo se esiste una base giuridica valida a norma dell’articolo 6, paragrafo 1, del GDPR; 7) il titolare dei dati potrà utilizzare i dati non personali generati dall’uso di un prodotto o di un servizio correlato solo sulla base di un accordo contrattuale con l’utente, mai però al fine di ottenere informazioni sulla situazione economica, sulle risorse e sui metodi di produzione o sull’utilizzo da parte dell’utente che potrebbero compromettere la sua posizione commerciale nei mercati in cui l’utente è attivo.

L'art. 5 del DA, che regola il diritto dell'utente di condividere i dati con terzi, stabilisce ora il necessario rispetto di alcune condizioni che riproducono, in buona sostanza, quelle già previste dall'art. 3. Mentre, sono state apportate alcune modifiche all'art. 6 del DA al fine di disciplinare il possibile scenario in cui l'utente non coincida con l'interessato, non previsto nell'originaria proposta della Commissione europea.

All'art. 7 del DA, infine, è stato precisato che gli obblighi di cui al Capo II non si applicano neppure ai “*dati generati dall'uso di prodotti fabbricati o di servizi correlati forniti da imprese che si qualificano come medie imprese*” (art. 7(1) DA).

Il titolo del **Capo III** è stato poi modificato in “*Obblighi orizzontali per i titolari di dati tenuti per legge a mettere a disposizione i dati nei rapporti tra imprese*”, al fine di rendere chiaro che gli obblighi ivi contenuti sono di natura orizzontale.

Il *compromise text* ha previsto poi alcune modifiche all'art. 8 del DA, al fine di alleggerire il linguaggio della originaria Proposta di Data Act, per non imporre in capo al titolare dei dati l'onere (eccessivamente gravoso) di dimostrare che non vi è stata discriminazione del destinatario dei dati. La disposizione in parola, infatti, ora prevede semplicemente che “*il titolare dei dati dovrà senza indebito ritardo fornire al destinatario dei dati, su richiesta di questo, informazioni che dimostrino l'assenza di discriminazioni*”. Inoltre, è stato chiarito che non è richiesto al titolare dei dati di condividere segreti commerciali con il destinatario dei dati, a meno che ciò non sia previsto dalla legge.

All'art. 9(2), invece, è stato chiarito che – come anche indicato all'art. 7(1) del DA – quando il destinatario sia una micro, piccola o media impresa, i principi sanciti nella Proposta di Data Act in relazione a tali tipologie di imprese valgono a condizione che esse non abbiano imprese connesse o collegate, secondo la definizione di cui all'articolo 3 dell'allegato alla raccomandazione 2003/361/CE, che non si qualificano come micro, piccole o medie imprese.

All'art. 10 del DA – che disciplina il meccanismo di risoluzione delle controversie tra titolari dei dati e destinatari di questi – è stato aggiunto il nuovo paragrafo (7a), con il quale si è previsto che “[g]li organi di risoluzione delle controversie rendono pubbliche le relazioni annuali di attività” e che il “*rapporto annuale comprende in particolare le seguenti informazioni: (a) il numero delle controversie decise; (b) il risultato di tali controversie; (c) il tempo medio richiesto al fine di risolvere tali controversie; (d) problemi comuni che si verificano frequentemente e che portano a controversie tra le parti; tali informazioni possono essere accompagnate da raccomandazioni su come evitare o risolvere tali problemi, al fine di facilitare lo scambio di informazioni e di migliori pratiche*”.

L'articolo 11(2) del DA è stato, invece, modificato per tenere meglio conto di ciò che dovrebbe accadere in caso di utilizzo o divulgazione non autorizzati dei dati; mentre, è stato aggiunto l'art. 11(2a) al fine di estendere le salvaguardie di cui all'art. 11(2) anche agli utenti, qualora il destinatario dei dati abbia violato quanto previsto all'art. 6(2)(a) ovvero all'art. 6(2)(b) della Proposta di Data Act.

Il **Capo IV** del DA, ora rinominato “*Clausole contrattuali abusive relative all'accesso ai dati e al relativo utilizzo*”, non presenta invece novità di rilievo rispetto all'originaria proposta della Commissione, salvo un coordinamento con l'art. 7(1) – simile a quello di cui all'art. 9(2) – che chiarisce la sfera di applicabilità delle disposizioni racchiuse in tale articolo alle micro, piccole o medie imprese.

RICCARDO ALFONSI

<https://data.consilium.europa.eu/doc/document/ST-11194-2022-INIT/en/pdf>

2022/3(4)VR

### **La proposta di Regolamento UE sui requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali (c.d. Cyber Resilience Act)**

Il 15 settembre 2022 la Commissione europea ha presentato, con la comunicazione n. 454, il progetto di Reg. UE in materia di cybersicurezza per i prodotti digitali, c.d. *Cyber Resilience Act* (nel prosieguo, “proposta di regolamento” o “Cyber Resilience Act”).

Alla base della proposta di regolamento è il crescente numero di attacchi informatici che hanno raggiunto un costo globale di 5.5 trilioni nel 2021. Ciò sarebbe da ricondurre essenzialmente a due fattori: *a)* un livello di sicurezza informatica generalmente basso, dovuto in parte alle insufficienze degli aggiornamenti; *b)* una scarsa alfabetizzazione digitale dell’utenza, che ostacola la scelta consapevole dei prodotti e il loro uso prudente. Inoltre, in ambienti interconnessi, gli incidenti riguardanti il singolo prodotto possono propagarsi con estrema rapidità, causando gravi interruzioni delle attività economiche e sociali o, financo, mettendo a rischio la vita umana. La dimensione globale dei mercati dei prodotti con elementi digitali, poi, comporta che la maggior parte di essi non sono attualmente soggetti ad alcuna regolazione europea sulla sicurezza informatica. È il caso, in particolare, dei *software* non incorporati, sovente bersaglio di attacchi di rilevante entità.

Come esplicitato nella comunicazione della Commissione “*Plasmare il futuro digitale dell’Europa*” del 19 febbraio 2020 (COM (2020) 67 definitivo), la cybersicurezza è uno dei quattro pilastri – oltre alla protezione dei dati, ai diritti fondamentali e alla sicurezza (dei prodotti) – per una società digitale in cui l’innovazione sia promossa entro confini sicuri ed etici.

Per tali ragioni, i due obiettivi principali della proposta di regolamento sono: creare le condizioni affinché siano sviluppati prodotti digitali la cui sicurezza perduri lungo tutto il loro ciclo di vita e promuovere la sicurezza informatica come elemento chiave per la scelta e l’utilizzo di prodotti digitali (v. Considerando 2). Da questi, si diramano quattro obiettivi specifici: *i)* assicurare un’implementazione degli standard di sicurezza sin dalla fase di progettazione e sviluppo; *ii)* fornire un quadro legislativo coerente in materia, per agevolare la conformità; *iii)* promuovere la trasparenza; *iv)* consentire alle imprese e ai consumatori di utilizzare i prodotti con elementi digitali in modo sicuro (v. Considerando 8).

L’intervento si impone anche in considerazione della frammentarietà e della lacunosità del quadro legislativo esistente. La frammentarietà è data dall’assommarsi delle dir. nn. 2013/40/UE (relativa agli attacchi contro i sistemi di informazione), 2016/1148/UE (c.d. NIS, sulla sicurezza delle reti e dei sistemi informativi), la futura Dir. NIS II e il Reg. 2019/881/UE (relativo all’ENISA, l’Agenzia dell’Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell’informazione e della comunicazione) (v. Considerando 4). La lacunosità deriva dall’assenza di prescrizioni specifiche per la sicurezza dei prodotti con elementi digitali, solo episodicamente contemplate da alcune discipline speciali (v. Considerando 3). Lungo tali direttrici, la proposta si coordina coi regimi in vigore, inglobando l’ambito di applicazione materiale del Reg. 2022/30/UE e stabilendo requisiti essenzialmente riproduttivi degli elementi cui all’art. 3, par. 3, lett. *d)*, *e)*, *f)* della dir. 2014/53/UE.

Ciò premesso, sul piano contenutistico la proposta si compone di 71 Considerando e di 57 articoli, distribuiti lungo 8 Capitoli.

Il Capitolo I delimita anzitutto l'oggetto (art. 1), che si articola in: *a*) norme per l'immissione sul mercato di prodotti con elementi digitali, al fine di garantirne la cybersicurezza; *b*) requisiti essenziali di progettazione, sviluppo e produzione e relativi obblighi per gli operatori economici *c*) requisiti essenziali per i processi di gestione delle vulnerabilità messi in atto dai produttori per garantire la sicurezza informatica dei prodotti con elementi digitali durante l'intero ciclo di vita e relativi obblighi per gli operatori economici; *d*) norme sulla sorveglianza del mercato e sull'applicazione della disciplina in oggetto.

Quanto all'ambito applicativo (art. 2), il regolamento dovrà applicarsi a tutti i prodotti con elementi digitali il cui uso previsto o ragionevolmente prevedibile include una connessione logica o fisica diretta o indiretta di dati a un dispositivo o a una rete. Ai sensi dell'art. 3, parr. 10 e 11, per "connessione logica" si intende una rappresentazione virtuale di una connessione dati implementata attraverso un'interfaccia *software*; la "connessione fisica", invece, è definita come qualsiasi connessione tra sistemi informativi elettronici o componenti realizzata con mezzi fisici, anche attraverso interfacce elettriche o meccaniche, fili o onde radio. Restano esclusi i prodotti disciplinati dal Reg. 2017/745/UE (relativo ai dispositivi medici), dal Reg. 2017/746/UE (relativo ai dispositivi medico-diagnostici *in vitro*), poiché prevedono entrambi requisiti relativi ai dispositivi, anche per quanto riguarda il *software*, e obblighi generali per i fabbricanti che riguardano l'intero ciclo di vita dei prodotti, nonché procedure di valutazione della conformità (v. Considerando 14). Inoltre, la proposta non si applicherà ai prodotti con elementi digitali certificati in conformità al Reg. 2018/1139/UE (recante norme comuni in materia di aviazione civile) né a quelli ai cui fa riferimento il Reg. 2019/2144/UE (sui requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada). Sono sottratti al regime in oggetto anche i prodotti sviluppati esclusivamente per scopi di sicurezza nazionale o militari e quelli specificamente progettati per elaborare informazioni classificate. Da ultimo, la promozione della ricerca e dell'innovazione dovrebbe portare a escludere dal perimetro tracciato anche i *software* liberi e *open-source* sviluppati o forniti al di fuori di un'attività commerciale, e in particolari quelli condivisi apertamente e liberamente accessibili, utilizzabili, modificabili e ridistribuibili (Considerando 10).

Il combinato disposto degli artt. 4 e 5 testimonia la linea di politica del diritto seguita: premessa la libera circolazione dei prodotti con elementi digitali, si prescrivono una serie puntuale di requisiti essenziali per la conformità (Sez. I, All. I) di questi e dei relativi processi messi in atto dai produttori (Sez. II, All. I).

Un regime di maggior rigore è approntato all'art. 6 per i prodotti con elementi digitali assunti come critici, ossia quelli elencati all'All. III e *ivi* suddivisi in due classi di rischio crescenti, a seconda dell'impatto delle potenziali vulnerabilità sul piano della cybersicurezza (v. Considerando 26). Alla Commissione è conferito il potere di modificare la lista, includendo categorie nuove e/o eliminandone alcune, entro parametri predeterminati. I prodotti critici con elementi digitali sono soggetti alle procedure di valutazione di conformità di cui all'art. 24, par. 2 e 3. Alla Commissione è inoltre conferito il potere di adottare atti delegati integrativi, specificando le classi di prodotti altamente critici per i quali i produttori, per dimostrare la conformità all'All. I, sono obbligati al previo ottenimento del certificato europeo di cui al Reg. 2019/881/UE.

Infine, va evidenziato il raccordo con l'attuale quadro normativo europeo relativo ai prodotti (v. Considerando 16) e con le proposte legislative, come l'*Artificial Intelligence Act* (21.4.2021 COM (2021) 206 final). In linea con le indicazioni generali dei Considerando 14 e 29, i prodotti con elementi digitali classificati come sistemi di IA ad alto rischio *ex art. 6*

AIA, che rientrano nell'ambito di applicazione della proposta in analisi e soddisfano i requisiti essenziali di cui alle Sez. I e II dell'All. I, sono considerati conformi ai requisiti relativi alla sicurezza informatica di cui all'art. 15 AIA e seguono la procedura di cui all'art. 43 AIA (art. 8).

Snodo centrale del progetto di regolamento è, senza dubbio, il Capitolo II. Esso condensa una serie di obblighi prescritti agli operatori economici – produttori, rappresentanti autorizzati, importatori, distributori o qualsiasi altra persona fisica o giuridica soggetta agli obblighi stabiliti dal regolamento (art. 3, n. 17) – graduati secondo la loro allocazione nella catena di fornitura e le loro conseguenti responsabilità. A livello generale, i prodotti con elementi digitali possono essere immessi sul mercato solo se forniti in modo corretto, opportunamente installati, sottoposti a manutenzione e utilizzati per lo scopo previsto o in condizioni ragionevolmente prevedibili.

Più precisamente, ai sensi dell'art. 10 della proposta i produttori devono garantire che la progettazione, lo sviluppo e la produzione sia conforme ai requisiti essenziali di cui alla Sez. I dell'All. I, effettuando una previa valutazione individuale dei rischi di cybersicurezza e tenendo conto dei relativi risultati nelle fasi descritte. Particolare importanza rivestono gli obblighi di documentazione: tutti i dati pertinenti o i dettagli dei mezzi utilizzati per garantire che il prodotto e i processi messi in atto dal fabbricante siano conformi ai requisiti essenziali di cui all'All. I, oltre agli esiti delle verifiche anzidette, sono da includere nella documentazione tecnica *ex art.* 23, che deve precedere l'immissione sul mercato. Inoltre, va documentato sistematicamente qualsiasi aspetto rilevante di cybersicurezza relativo al prodotto, provvedendo, ove le risultanze lo richiedano, ad aggiornare la valutazione di rischio. Tra gli adempimenti, spicca poi l'esecuzione delle procedure di valutazione della conformità, di cui all'art. 24, che, ove concluse con esito positivo, consentono di redigere la dichiarazione di conformità CE (art. 20) e l'apposizione della relativa marcatura (art. 22). Seguono poi i doveri informativi: le informazioni e le istruzioni di cui all'All. II accompagnano costantemente il prodotto e devono essere chiare, comprensibili, intelleggibili e leggibili. Tutti i dati e i documenti necessari a dimostrare la conformità ai requisiti essenziali di cui all'All. I devono essere forniti all'autorità di vigilanza del mercato, su richiesta motivata di essa. Completano il quadro gli obblighi di comunicazione. Ai sensi dell'art. 11 della proposta di regolamento, i produttori devono notificare all'ENISA, senza indebito ritardo e in ogni caso entro 24 ore dal momento in cui ne hanno conoscenza, qualsiasi vulnerabilità attivamente sfruttata contenuta nel prodotto con elementi digitali e qualsiasi incidente che possa minarne la sicurezza. Degli incidenti, nonché delle eventuali misure correttive esperibili, deve essere prontamente informata anche l'utenza.

Le obbligazioni dei rappresentanti autorizzati, nominati dal fabbricante mediante mandato scritto, sono assai più ridotte, e il legislatore si premura vieppiù di attribuire ad essi una posizione di interlocutore qualificato dell'autorità di vigilanza del mercato (art. 12).

Agli importatori è affidato, dall'art. 13 della proposta di regolamento, un ruolo – per così dire – di controllo e garanzia. Essi, per prima cosa, sono tenuti a immettere sul mercato solo prodotti con elementi digitali conformi ai requisiti essenziali di cui alla Sez. I dell'All. I e i cui processi messi in atto dal produttore sono conformi ai requisiti essenziali di cui alla Sez. II dell'All. I. Prima dell'immissione sul mercato, tali soggetti devono garantire l'esatta esecuzione delle procedure di valutazione della conformità *ex art.* 24, la redazione della documentazione tecnica e l'apposizione della marcatura CE di cui all'art. 22, assieme alle informazioni e dalle istruzioni di cui all'All. II., da parte del fabbricante. Qualora l'importatore abbia fondati motivi di dubbio sulla conformità del prodotto o dei processi, gli è fatto divieto di immetterlo fino a quando entrambi sono resi conformi. Ove tale diagnosi sopravvenga all'immissione sul mercato, è prescritta l'adozione delle misure correttive

necessarie o, se del caso, il richiamo o il ritiro del prodotto. Da ultimi, vanno menzionati i doveri di segnalazione delle vulnerabilità rilevate al fabbricante e a questi e all'autorità di vigilanza del mercato degli Stati membri presso cui il prodotto è stato messo in circolazione, ove si tratti di rischi significativi per la sicurezza informatica.

La platea dei destinatari qualificati termina con i distributori, la cui posizione testimonia un incremento dei doveri di controllo e garanzia proporzionale all'allungamento della catena. A fronte di un generico obbligo di agire con la dovuta attenzione in relazione ai requisiti prescritti, tali operatori sono tenuti, prima della messa a disposizione di un prodotto con elementi digitali, a verificare la sussistenza del marchio CE e l'effettivo assolvimento da parte del produttore e dell'importatore degli adempimenti previsti, rispettivamente, dagli artt. 10, par. 10 e 11, e 13, par. 4. Per il resto, l'art. 14 ricalca fedelmente la disciplina predisposta per gli importatori alla disposizione precedente, quanto ai fondati motivi di dubbio sulla conformità, originari o sopravvenuti, ai doveri di avviso, correzione e intervento.

Merita, infine, segnalare che gli importatori e i distributori sono equiparati ai produttori, con conseguente soggezione alle prescrizioni *ex* artt. 10 e 11, par. 1, 2, 4 e 7, qualora immettano sul mercato un prodotto con elementi digitali con il proprio nome o marchio o vi effettuino una modifica sostanziale (art. 15; cfr. Considerando 24). Solo in quest'ultimo caso, l'estensione comprende anche gli operatori economici non qualificati, ossia, in generale, qualunque persona fisica o giuridica (art. 16).

Il Capitolo III della proposta di regolamento è dedicato alla conformità e si apre, all'art. 18, con un'importante regola presuntiva. Anzitutto, i prodotti con elementi digitali conformi agli *standard* europei armonizzati o a parti di essi si presumono conformi ai requisiti essenziali richiesti dall'All. I della proposta. Altrettanto vale per i prodotti e i processi digitali conformi alle specifiche comuni di cui all'art. 19 o per i quali è stata rilasciata una dichiarazione di conformità UE o un certificato emesso nell'ambito di un sistema europeo di certificazione della cybersicurezza ai sensi del Reg. 2019/881/UE, limitatamente alle caratteristiche *in* contemplate (v. Considerando 39). Giova, inoltre, segnalare che: *i*) le evocate specifiche comuni *ex* art. 19 assumono una veste essenzialmente suppletiva, potendo essere adottate dalla Commissione mediante atti di esecuzione se le norme armonizzate non esistono o sono insufficienti, se vi sono ritardi ingiustificati nella procedura di standardizzazione o se la richiesta della Commissione non è stata accettata dalle organizzazioni europee di standardizzazione; *ii*) la dichiarazione di conformità UE segue il modello di cui all'All. IV, contiene gli elementi specificati nelle pertinenti procedure di valutazione della conformità di cui all'Allegato VI, va sottoposta ad aggiornamento costante e, soprattutto, comporta per il produttore l'assunzione della responsabilità sulla conformità del prodotto (art. 20); *iii*) il marchio CE va apposto in modo visibile, leggibile e indelebile sul prodotto con elementi digitali o, se ciò non è possibile o non può garantirsi, sull'imballaggio e sulla dichiarazione di conformità UE o su di essa e sul sito web per i prodotti *software* (art. 22).

Al fine di garantire un elevato livello di sicurezza informatica e la fiducia di tutte le parti interessate, particolare enfasi è posta al Capitolo IV sul raccordo con gli organismi di valutazione della conformità (cc.dd. organismi notificati) e, più a monte, con le autorità nazionali di notifica. In quest'ottica, gli Stati membri designano un'autorità responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione e la notifica degli organismi di valutazione della conformità, nonché per il monitoraggio degli stessi, in linea con la decisione 768/2008/CE e secondo i requisiti fissati nella proposta (art. 27). Gli organismi autorizzati e costituiti secondo il dettato dell'art. 29 eseguono le valutazioni di conformità secondo le procedure di cui all'art. 24 e all'All. VI in modo proporzionato e rigoroso. Ove abbiano ragione di ritenere che le prescrizioni di cui all'All. I o alle corrispondenti norme armonizzate o alle specifiche comuni *ex* art. 19 non siano state

rispettate dal produttore, detti organismi negano il rilascio del certificato di conformità e sollecitano l'adozione delle pertinenti misure correttive. Se le criticità emergono durante il monitoraggio successivo al rilascio di un certificato, alla richiesta *de qua* può seguire la sospensione o il ritiro del certificato. Tali ultime ipotesi, assieme alla limitazione, costituiscono via obbligata in caso di mancata assunzione delle misure correttive o di fallimento delle stesse.

Altro modulo fondamentale del progetto riguarda la sorveglianza del mercato e l'*enforcement*, di cui al Capitolo V (v. Considerando 54). Al fine di garantire l'effettività delle misure in analisi, ciascuno Stato membro designa una o più autorità di vigilanza del mercato, con cui gli operatori economici sono tenuti a collaborare proficuamente. Inoltre, ai prodotti con elementi digitali rientranti nell'ambito di applicazione della proposta si applica il Reg. 2019/1020/UE (sulla vigilanza del mercato e sulla conformità dei prodotti) (v. Considerando 55). Particolari cautele sono riservate ai prodotti con elementi digitali che presentano un rischio significativo di cybersicurezza (artt. 45 e 46).

Da ultimo, deve farsi cenno al Capitolo VII, segnalando il dovere generale di riservatezza sulle informazioni e sui dati ottenuti dai soggetti interessati nello svolgimento dei loro compiti e delle loro attività (art. 52) e la disciplina delle sanzioni *ex art.* 53. Su quest'ultimo aspetto, la proposta fissa soglie massime e affida la concreta ponderazione alla discrezionalità dei legislazioni nazionali (v. Considerando 62): l'inosservanza dei requisiti essenziali di cui all'All. I e degli obblighi di cui agli artt. 10 e 11 è soggetta a sanzioni amministrative pecuniarie fino a 15 milioni di euro o, se il trasgressore è un'impresa, fino al 2,5% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore; la violazione di qualsiasi altro obbligo conduce a sanzioni amministrative pecuniarie fino a 10.000.000 di euro o, se il trasgressore è un'impresa, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Può concludersi riportando l'indicazione di cui al Considerando 68, che fa trasparire un indirizzo regolatorio flessibile, quasi reso *rebus sic stantibus*, per cui la Commissione dovrebbe riesaminare periodicamente la disciplina in analisi, in consultazione con le parti interessate, valutando la necessità di modifiche alla luce dell'evoluzione delle condizioni sociali, politiche, tecnologiche o di mercato.

VALENTINO RAVAGNANI

<https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>

2022/3(5)EMI

### **Verso il regolamento europeo di progettazione eco-sostenibile dei dispositivi mobili tecnologici.**

Lo scorso 28 settembre 2022 si è conclusa la fase (c.d. *draft act*) dedicata all'invio di commenti in merito alla proposta di Regolamento europeo in materia di progettazione eco-sostenibile dei dispositivi mobili tecnologici («*laying down ecodesign requirements for mobile phones, cordless phones and slate tablets pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending*») (nel prosieguo, anche “Proposta di Regolamento” o “Proposta”). L'iniziativa euro-unitaria si inserisce nel più ampio *Piano d'azione per l'economia circolare*, presentato nel 2020 (*Circular Economy Action Plan - For a cleaner and more competitive Europe*) nonché con gli obiettivi del *Green Deal* europeo in materia di uso efficiente delle risorse.

Con questa proposta, la Commissione europea intende stabilire, in particolare, nuove norme in materia di progettazione e di produzione eco-compatibile e sostenibile dei dispositivi mobili, quali cellulari, telefoni e tablet. La proposta di regolamento rappresenta un altro passo di un lungo percorso avviato, prima, con l'istituzione del *Piano di lavoro sulla progettazione ecocompatibile* (2016-2019) e, poi, con la pubblicazione di un uno studio preparatorio in tema di progettazione ecocompatibile dei telefoni, smartphone e tablet, che già auspicava l'introduzione di norme specifiche per l'*ecodesign* e l'etichettatura energetica di questi prodotti tecnologici. Le regole contenute nella proposta di regolamento mirano a garantire una superiore efficienza energetica dei dispositivi prodotti e soprattutto una maggiore durata, una più facile riparabilità, una modificabilità in caso di errori o malfunzionamenti ed anche delle più elevate possibilità di riutilizzo o di riciclo. Così facendo, la proposta intende concorrere a un miglioramento delle prestazioni ambientali dei dispositivi tecnologici in termini di consumo di energia e di acqua, di livelli di emissione di CO<sub>2</sub> e di efficienza dei materiali impiegati nella produzione, nonché favorire il riutilizzo e lo smaltimento dei prodotti nell'ottica di una economia ecosostenibile e circolare.

La proposta va ad ampliare la linea tracciata precedentemente dalla Direttiva 2009/125/CE relativa all'istituzione di un quadro europeo per l'elaborazione di regole specifiche per la progettazione sostenibile dei prodotti, da un lato, impedendo a dispositivi poco efficienti da un punto di vista energetico di essere immessi sul mercato e, dall'altro, concedendo ai consumatori la possibilità di compiere scelte maggiormente consapevoli. Per realizzare i suddetti obiettivi, si mira a costituire una cornice regolatoria orientata alla sostenibilità ambientale ed energetica dei prodotti e dispositivi tecnologici immessi sul mercato e che guarda all'intero ciclo del prodotto, dalla progettazione all'immissione nel mercato con le successive fasi di riparazione o riciclo.

La Proposta di Regolamento comprende una bozza di regolamento e sei allegati di supporto e si sviluppa secondo tre chiare linee direttive:

- a) immettere sul mercato dispositivi duraturi ed efficienti dal punto di vista energetico;
- b) assicurare ai consumatori un facile accesso alla riparazione, all'aggiornamento e alla manutenzione dei dispositivi mobili;
- c) semplificare i processi di riuso e riciclo dei prodotti.

Gli **artt. 1-2** della Proposta specificano l'ambito applicativo del regolamento e le definizioni rilevanti a tal fine, escludendo alcune tipologie di dispositivi mobili («(a) *mobile phones and tablets with a flexible main display which the user can unroll and roll up partly or fully*; (b) *smartphones designed for high security communications*»). L'**art. 2**, specificatamente, fornisce le definizioni tecniche di *mobile phones*, *cordless phones* e *slate tablets*, che devono presentare determinati standard qualitativi ai fini della bozza di Regolamento. Le tre categorie di dispositivi, a cui si applica la Proposta, sono accumulate dal fatto di essere tutti dispositivi mobili con modalità di telecomunicazione a distanza ed informatica. L'**Allegato I** delimita il perimetro applicativo della proposta, attraverso l'elencazione di diversi dispositivi tecnologici impiegabili, le cui definizioni forniscono un quadro chiaro di applicazione della Proposta.

L'**art. 3**, invece, rimanda in merito agli standard tecnici e di eco-design da seguire all'**Allegato II** che contiene le diverse regole specifiche per i singoli dispositivi tecnologici impiegati.

In particolare, come si evince dall'**Allegato II** («*Ecodesign requirements*»), la Commissione impone limiti (minimi) di durata – per contrastare anche il fenomeno della c.d. obsolescenza programmata – sia per quanto riguarda l'uso dei dispositivi sia per quanto concerne la fase di manutenzione e riparazione. Il prodotto, infatti, deve garantire al consumatore un uso minimo di cinque anni dalla sua immissione nel mercato e deve essere assicurato l'accesso ai manuali di manutenzione per i sette anni successivi alla prima cessione del prodotto.

Nello specifico, così come esplicitato negli allegati tecnici, per facilitare il riciclo, si dovranno mettere pubblicamente a disposizione del singolo consumatore (per 15 anni a seguito dell'immissione sul mercato del prodotto) le istruzioni di manutenzione e accesso al software, con specifici passaggi tecnico-informatici da seguire. La proposta, inoltre, si concentra particolarmente sulla fase di riparazione del prodotto, entrando nel merito delle modalità di riparazione e imponendo standard qualitativi ai materiali utilizzati. In aggiunta a ciò, si mira a facilitare il procedimento per richiedere la riparazione del dispositivo, attraverso l'istituzione di procedure semplificate online.

L'art. 4, in merito alla valutazione di conformità, richiama l'art. 8 della Direttiva 2009/125/EC con l'obiettivo di rendere uniformi i processi valutativi dei prodotti tecnologici presenti nel mercato.

Ai fini delle procedure di controllo sul mercato («*Verification procedure for market surveillance purposes*»), l'art. 5 fa da ponte tra le indicazioni contenute all'interno dell'Allegato IV e quanto disposto dall'art. 3 (2) della Direttiva 2009/125/EC (che prevede l'intervento dell'Autorità nazionali responsabili della sorveglianza sul mercato).

Inoltre, come mette in evidenza l'art. 6 della bozza di regolamento, le nuove regole imporranno ulteriori standard e caratteristiche tecniche («*measures against circumvention*») ai dispositivi tecnologici immessi sul mercato, per garantire le già menzionate esigenze di sostenibilità energetica e di design eco-compatibile.

L'art. 7, invece, stabilisce che i riferimenti ai c.d. *indicative benchmarks* sono contenuti all'interno dell'Allegato V. Difatti, essi dovranno essere idonei a resistere ad urti, graffi od altro tipo di impatti, nonché ad acqua e polvere, oltre a dover rispettare specifici requisiti minimi in relazione alle batterie impiegate.

Infine, la disposizione dell'art. 8 prevede un aggiornamento («*review*») della proposta alla luce dell'evoluzione tecnologica del mercato, da sottoporre al c.d. *Consultation Forum* istituito in virtù dell'art. 14 del Regolamento (UE) 2017/1369.

In conclusione, si è vicini all'approvazione di una importante iniziativa in ambito europeo che consolida la posizione (d'avanguardia) dell'Unione a favore della costituzione di un mercato unico sempre più sostenibile ed orientato al rispetto dell'ambiente, di standard energetici minimi – ad oggi, questione centrale a livello nazionale ed internazionale – e di obblighi informativi coerenti che diano la possibilità di scelte consapevoli ed informate ai consumatori.

ENZO MARIA INCUTTI

[https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12797-Progettazione-sostenibile-di-telefoni-cellulari-e-tablet-progettazione-ecocompatibile\\_it](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12797-Progettazione-sostenibile-di-telefoni-cellulari-e-tablet-progettazione-ecocompatibile_it)

2022/3(6)ES

### **Gli ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection.**

L'8 settembre 2022 l'*European Law Institute* (c.d. ELI) ha emanato il *draft* dei *Principles on Blockchain Technology, Smart Contracts and Consumer Protection* (di seguito anche i “**Principi**” o il “**Framework**”) la cui gestazione era iniziata sin dal 2018.

La Distributed Ledgers Technology (c.d. “DLT”), nonché la blockchain e gli smart contracts che sono basati su di essa, sono fenomeni che evolvono rapidamente complicando

e ritardando l'elaborazione di principi, e soprattutto di norme, organici in materia. Nondimeno, tale evoluzione solleva numerosi interrogativi a cui è difficile dare risposta anche in virtù dell'assenza di un framework giuridico di riferimento sebbene, recentemente, l'Unione Europea abbia emanato diverse proposte legislative. Ci si riferisce al **Data Governance Act** (su cui v. notizia [2021/4\(4\)RA](#) e notizia [2022/2\(1\)RA](#)), al **Digital Finance Package** (su cui v. notizia [2022/2\(2\)BC](#)), all'**Artificial Intelligence Act** (su cui v. notizia [2021/2\(1\)SO](#)), al **Digital Services Act** (su cui v. notizia [2021/3\(1\)DI](#)), al **Digital Market Act** e al **Data Act** (su cui v. notizie [2022/1\(2\)RA](#) e [2022/1\(4\)SO](#)). Gli studi giuridici sulla blockchain e sugli smart contracts, peraltro, non sono ancora del tutto maturi, complice anche la continua evoluzione del fenomeno. I Reporters, dunque, hanno tentato di sviluppare quel framework giuridico sinora mancante, nell'ottica di fornire soluzioni armonizzate almeno tra gli Stati membri dell'UE, concentrandosi sull'elaborazione di un ristretto numero di principi e focalizzandosi, in particolare, sulla tutela dei consumatori. Il Framework è diviso in due parti: la prima dedicata ai principi di carattere generale; la seconda alla tutela dei consumatori coinvolti in smart contracts. Ogni Principio, a sua volta, si articola in una black letter rule e in note esplicative.

Il Framework segue un approccio basato sulla neutralità tecnologica e sull'equivalenza funzionale. Per neutralità tecnologica si intende una soluzione applicabile a diversi tipi di rapporti giuridici a prescindere dal tipo di tecnologia utilizzata. Per equivalenza funzionale ci si riferisce al fenomeno per cui un accordo vincolante concluso offline debba avere lo stesso valore giuridico di uno concluso sulla blockchain. Il Framework, inoltre, propone soluzioni giuridiche basate sul funzionamento in concreto della tecnologia blockchain (c.d. "Use-Case Approach").

Riguardo alla **Parte I**, va detto che il **Principio 1 a)** identifica l'ambito di applicazione territoriale del Framework individuandolo sia negli Stati membri dell'UE sia in quelli extra UE. Il Principio 1 let. c), inoltre, chiarisce che il Framework detta norme valide solo per le transazioni realizzate tramite la blockchain e gli smart contracts (di seguito le "**Transazioni**") e non per il funzionamento di tali tecnologie. I Principi, inoltre, si concentrano su tematiche di civil law e, in particolare, sulle transazioni commerciali. Sono esclusi dal loro ambito di applicazione la creazione di diritti reali, la proprietà, il risarcimento, questioni successorie, matrimoniali e di convivenza.

Sempre al Principio 1, la let. b) chiarisce che il Framework intende stabilire una concezione comune di blockchain e smart contract, guidare i professionisti nell'applicazione delle norme esistenti in materia, stimolare ulteriori sviluppi sull'argomento e informare il pubblico delle best practices di settore. Ovviamente, tali obiettivi impongono un coordinamento con le normative eventualmente esistenti in materia.

Il **Principio 2** let. a) distingue le tipologie di smart contracts in: 1) meri codici privi di valore giuridicamente vincolante; 2) strumenti per eseguire accordi raggiunti al di fuori di una blockchain (c.d. Off-Chain); 3) contratti vincolanti; 4) una fusione tra smart contract stesso e accordo Off-Chain, che impone di stabilire se il contratto sia stato concluso sulla blockchain (c.d. On-Chain) o Off-Chain.

La già menzionata classificazione degli smart contracts discende dai diversi tipi di blockchain esistenti. Quest'ultima, infatti, può essere pubblica o privata a seconda che tutti o solo alcune persone possano parteciparvi. Nondimeno, è possibile distinguere tra blockchain c.d. "permissioned" o "permissionless" a seconda che solo le persone specificamente autorizzate o meno possano eseguire transazioni. I partecipanti alla rete, inoltre, possono essere privati, imprese o enti pubblici.

Al netto di questioni classificatorie, però, occorre chiedersi se gli smart contracts possano costituire accordi giuridicamente vincolanti. La risposta al quesito presuppone un'indagine

caso per caso attenta alla natura delle parti coinvolte e alla tipologia di smart contract utilizzata, come afferma anche il **Principio 3**.

Ad ogni modo, gli smart contracts ben possono dare vita a contratti vincolanti e, in caso di disaccordo tra contratto concluso On-Chain (ossia concluso sulla blockchain) e Off-Chain, il Principio 2 let. a) 4) stabilisce che prevalga quest'ultimo.

Il **Principio 4** let a) stabilisce che alle transazioni realizzate sulla blockchain si applicano le stesse norme applicabili a quelle concluse Off-Chain, incluse quelle di diritto internazionale privato. Di conseguenza, è ammissibile pure la scelta di legge e del Foro competente (let. b) del Principio in commento). Il semplice fatto che la transazione avvenga tra i nodi di una rete che per definizione è decentralizzata, tuttavia, non costituisce un presupposto sufficiente ad applicare il diritto internazionale privato essendo comunque necessario un elemento di transnazionalità, il c.d. criterio di collegamento (let. c) del Principio in commento).

Il **Principio 5** è dedicato alla natura giuridica delle transazioni concluse sulla blockchain. Per affrontare il tema, i Reporters si sono basati sul Draft Common Frame of Reference (c.d. DCFR) che impone di effettuare una valutazione caso per caso considerando sia i soggetti della Transazione, che possono essere B2C, B2B o B2G, sia l'oggetto della medesima.

Il Principio afferma che una Transazione ben può costituire un'offerta, l'accettazione di un'offerta o altra dichiarazione con valore vincolante, così originandosi un accordo giuridicamente vincolante, laddove vi sia una manifestazione di volontà chiaramente riferibile ad una parte della Transazione.

Al riguardo, come fatto dal Framework, è utile rappresentare la posizione assai netta in favore della natura contrattuale delle transazioni concluse sulla blockchain della Court of Appeal di Singapore nel caso *Quoine Pte Ltd v B2C2 Ltd*, [2020] SGCA(I) 02. La sentenza, infatti, afferma: “*there is no reason why the normal rules should not apply just because a potential contract is a smart contract*”. Analogamente, il Report “Smart Legal Contracts” della English Law Commission datato novembre 2021, sostanzialmente facendo proprie le conclusioni della UK Jurisdiction Taskforce, dichiara: “*smart legal contracts can satisfy the requirements for a contract*”.

Il **Principio 6** prevede che le Transazioni siano efficaci a partire dal giorno stabilito dalle parti. Se queste non dispongono nulla, le transazioni On-Chain sono efficaci da quando il destinatario della proposta contrattuale viene a conoscenza di quest'ultima oppure la transazione è registrata sulla blockchain.

Il **Principio 7** è dedicato ai requisiti formali della Transazione e si basa sui concetti di equivalenza funzionale e neutralità tecnologica.

Innanzitutto, il Principio 7 let. a) stabilisce che laddove un ordinamento imponga dei requisiti di forma per un accordo, che siano replicati anche online, si deve ritenere che tali requisiti siano stati rispettati. Le successive lett. b) e c) del Principio in esame richiamano la nota distinzione tra “text form”, ossia atto scritto, e “written form”, ossia atto scritto e firmato, nata nel codice civile tedesco, il BGB.

Ora, la forma scritta è agevolmente replicabile sulla blockchain o negli smart contracts. Maggiori difficoltà, invece, presenta l'apposizione di una firma o il rispetto di una forma solenne. Eppure, il Principio 7 let. c) stabilisce che anche questi requisiti possono essere soddisfatti, qualora una Transazione: i) garantisca le stesse tutele previste per un contratto Off-Chain; ii) raggiunga l'obiettivo per cui sono stati imposti i requisiti formali e iii) soddisfi i dettami del Regolamento eIDAS.

Il **Principio 8** stabilisce che le parti possono scegliere la lingua di una Transazione.

In caso di contrasto tra la versione On-Chain e Off-Chain di un accordo, però, sorge una questione interpretativa sul linguaggio, naturale o informatico. In tal caso, il Framework non interviene dettando dei criteri interpretativi limitandosi a stabilire che sia la versione Off-Chain a prevalere (**Principio 9**).

Il Framework si occupa anche della risoluzione delle Transazioni stabilendo, al **Principio 10**, che laddove la legge applicabile preveda un diritto di risoluzione e questa sia esercitato da un contraente, esso si traduca in una transazione inversa rispetto a quella che si desidera risolvere (c.d. reverse transaction).

Eventuali controversie tra le parti di una Transazione possono essere rimesse ad un arbitrato (**Principio 11**). Sebbene tale soluzione sia stata sostenuta anche nel Report sul “Digital Dispute Resolution Rules” della UK Jurisdictional Taskforce, permangono alcuni interrogativi al riguardo, soprattutto laddove la normativa applicabile alla Transazione richieda la “classica” forma scritta della clausola compromissoria.

Il **Principio 12** prevede che le parti deboli di una Transazione debbano godere della medesima tutela di cui beneficerebbero in caso di accordo Off-Chain. Una transazione On-Chain, infatti, non può essere il mezzo per ridurre le tutele dei consumatori.

La **Parte II** del Framework detta una serie di principi proprio a tutela dei consumatori.

Come noto, l’art. 2 dir. 2019/771/UE definisce questi ultimi come “*qualsiasi persona fisica che ... agisca per fini che non rientrano nel quadro dell’attività commerciale, industriale, artigianale o professionale di tale persona*”. E’ ben possibile, tuttavia, che le imprese, soprattutto quelle medio piccole, si trovino in una situazione equiparabile a quella dei consumatori, ovvero di debolezza, nei propri rapporti commerciali. Di conseguenza, sebbene i Reporters affermino che il Framework è stato volutamente elaborato concentrandosi sul consumatore persona fisica, nulla vieta che esso possa applicarsi anche nei rapporti tra pari (c.d. Peer to Peer), ossia tra imprese.

Ciò detto, il **Principio 13** let. a) afferma chiaramente che la tutela dei consumatori non può essere pregiudicata dal fatto che una transazione avviene sulla blockchain. Facendo buon uso dei criteri di neutralità tecnologica ed equivalenza funzionale, il Principio 13 let. b) afferma che i consumatori hanno diritto alla medesima protezione per le transazioni concluse Off-Chain e On-Chain; “*l’uso della tecnologia BLOCKCHAIN o di uno SMART CONTRACT non dovrebbe privare i consumatori di alcun diritto*” (let. c)). Di conseguenza, le imprese che ricorrano agli smart contracts sono tenute ad assicurarsi che i consumatori possano esercitare i propri diritti come se si trattasse di una transazione Off-Chain. La circostanza per cui un rimedio giuridico sia troppo difficile da implementare sulla blockchain, infatti, non può consentire eccezioni alla tutela dei consumatori. Tale impostazione dei Principi tiene conto del fatto che le transazioni online sono spesso meno trasparenti e controllabili rispetto a quelle Off-Chain.

Sempre per tale motivo, il Principio 13 let. f) prevede che i consumatori, i quali in buona fede abbiano concluso una Transazione devono essere tutelati da eventuali pattuizioni Off-Chain, tra l’impresa che abbia stipulato la Transazione col consumatore e soggetti terzi, le quali pregiudichino i diritti della parte debole.

Il **Principio 14** ammette che nei contratti coi consumatori le parti possano scegliere la legge regolatrice dell’accordo e il Foro competente a risolvere eventuali controversie nascenti da esso senza, però, ledere i diritti dei consumatori.

Il **Principio 15** stabilisce, per quanto ci interessa, che i consumatori abbiano diritto a ricevere una copia scritta - nel linguaggio naturale - degli smart contracts, che, come noto, consistono in un codice informatico. La ratio di tale previsione è evitare che le Transazioni ledano gli interessi dei consumatori. Per questo motivo, i Reporters propongono anche due soluzioni per verificare che lo smart contract pregiudichi gli interessi dei soggetti deboli. La prima consiste nella conduzione di un audit sullo smart contract per assicurarsi che esso non leda i diritti fondamentali dei consumatori. La seconda soluzione, ispirato dall’art. 5 dir. 1993/13/CE s.m.i., impone che i termini contrattuali siano sempre redatti per iscritto in

forma intellegibile; in caso di dubbio sul significato di una pattuizione, però, prevale sempre l'interpretazione più favorevole al consumatore.

Il **Principio 16**, ispirato dai criteri di neutralità tecnologica ed equivalenza funzionale, rappresenta l'evoluzione dei precedenti Principi 8 e 13, laddove alle lett. a) e b) afferma che i consumatori, i quali concludano una Transazione hanno diritto alle stesse informazioni pre-contrattuali e post-contrattuali che avrebbero avuto se avessero concluso un classico contratto Off-Chain. Le successive lett. c) e d) del Principio, ricordano che tali informazioni debbano sempre essere disponibili per iscritto in linguaggio naturale. Nondimeno, al consumatore spetta un documento esplicativo delle previsioni dello smart contract. Laddove lo smart contract differisca dal suddetto documento, quest'ultimo prevarrà sul testo contrattuale.

Il **Principio 17** è dedicato al diritto di ripensamento e recesso.

Il consumatore ha diritto di essere informato dell'esistenza in suo favore di un periodo di ripensamento (c.d. "cooling-off period"), il quale ovviamente deve essere codificato nello smart contract, e che egli potrà esercitare ogni diritto connesso al menzionato periodo con una transazione tanto On-Chain, quanto Off-Chain. Per far sì che tale periodo di ripensamento sia effettivo, la let. b) del Principio in commento stabilisce che lo smart contract potrà produrre effetti solo dopo che sia decorso tale arco temporale senza che il consumatore abbia esercitato il diritto di recesso.

Quest'ultimo deve consistere in una transazione inversa che sostanzialmente annulla la precedente con cui il contratto era stato concluso (let. d) del Principio). Il consumatore deve altresì essere informato di eventuali diritti (e obblighi) connessi all'esercizio del recesso, qualora previsti dalla normativa applicabile, e che la transazione inversa abbia avuto luogo.

Il **Principio 18**, infine, è dedicato alle clausole vessatorie e stabilisce che i consumatori debbano godere di una tutela effettiva per le transazioni concluse sia On-Chain sia Off-Chain (let. a) del Principio 18). Di conseguenza, essi devono poter risolvere On-Chain (oltreché Off-Chain) un contratto concluso online. Altrimenti la protezione riconosciutagli sarebbe compromessa.

Il Principio in commento alla let. b), inoltre, precisa che la previsione per cui un contratto può essere concluso solo online non è di per sé vessatoria.

Assai utilmente, poi, la let. d) del Principio 18 stabilisce che la dir. 1993/13/CE s.m.i. e l'acquis communautaire formatosi riguardo alla suddetta direttiva si applicano alle clausole vessatorie degli smart contracts. In presenza di clausole vessatorie self executing, inoltre, il consumatore ha diritto alla ricodifica dello smart contract per eliminare la clausola in commento.

La let. e) del Principio 18, infine, stabilisce che laddove una clausola sia stata dichiarata vessatoria in una class action, allora il professionista deve eliminarla da tutti gli smart contracts che la prevedano.

EMANUELE STABILE

[https://www.europeanlawinstitute.eu/fileadmin/user\\_upload/p\\_eli/Publications/ELI Principles on Blockchain Technology Smart Contracts and Consumer Protection Council Draft.pdf](https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology_Smart_Contracts_and_Consumer_Protection_Council_Draft.pdf)

**Il parere congiunto EDPB-EDPS sulla proposta di regolamento della Commissione Europea del 11.05.2022 che stabilisce norme per prevenire e combattere l'abuso sessuale dei minori.**

Il 28 luglio 2022 l'European Data Protection Board ("EDPB", ex WP 29) e l'European Data Protection Supervisor ("EDPS") hanno pubblicato, ai sensi dell'art. 42, paragrafo 2, del Regolamento UE n. 2018/1725, il parere congiunto n. 4/2022 (il "parere") sulla proposta di regolamento della Commissione europea del 11.5.2022 che stabilisce norme per prevenire e combattere l'abuso sessuale dei minori ("proposta di regolamento).

La proposta di regolamento è destinata a sostituire il regolamento (UE) 2021/1232, entrato in vigore nel 2021 come misura temporanea per consentire ad alcune categorie di fornitori di servizi di individuare e segnalare abusi sessuali su minori online e di rimuovere dai loro servizi materiale pedopornografico, nel rispetto della normativa europea sulla protezione dei dati personali.

Tale proposta di regolamento impone obblighi qualificati ai fornitori di servizi di hosting, di servizi di comunicazione interpersonale e di altri servizi, in merito alla individuazione, la segnalazione, la rimozione e il blocco di materiale online noto e nuovo relativo ad abusi sessuali su minori ("CSAM"), nonché l'adescamento di minori. Tali fornitori saranno obbligati a valutare e mitigare il rischio di abuso sui loro servizi e qualsiasi misura adottata dovrà essere proporzionata e soggetta ad adeguate garanzie. Il regolamento proposto istituirà anche un Centro Europeo sugli abusi sessuali sui minori e delle autorità nazionali di coordinamento, che faciliteranno l'attuazione del regolamento proposto.

Nel parere, l'EDPB e l'EDPS condividono il loro punto di vista sulla questione di come trovare il giusto equilibrio tra il diritto alla riservatezza delle comunicazioni e della vita privata e familiare, il diritto alla protezione dei dati personali (artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea) e gli sforzi per affrontare l'abuso sessuale dei minori online.

I due enti sollevano una serie di preoccupazioni in merito alla proposta di regolamento, in particolare per quanto riguarda la questione se le interferenze con i diritti fondamentali che prevede siano "necessarie" e "proporzionate" e come tali termini debbano essere interpretati in questo contesto. Nel fare ciò, vengono richiamate decisioni della CGUE relative a misure legislative che violano i diritti fondamentali in settori quali la giustizia penale e la sicurezza nazionale, tra cui i casi *Digital Rights Ireland*, *Tele2Sverige* e *Watson*, *Schrems* e *La Quadrature du Net*. La proposta di regolamento della Commissione potrebbe presentare più rischi per gli individui e per la società in generale che per i criminali perseguiti da CSAM; il rischio è che la proposta di regolamento possa diventare la base per una scansione generalizzata e indiscriminata dei contenuti di praticamente tutti i tipi di comunicazioni elettroniche.

Tanto premesso, l'EDPB e l'EDPS hanno espresso, al riguardo, una serie di raccomandazioni e osservazioni, di seguito sintetizzate:

La proposta di regolamento abrogerebbe il regolamento 2021/1232 ed eliminerebbe l'attuale regime in base al quale è consentito il trattamento dei dati personali al fine di individuare e rimuovere gli abusi sessuali su minori online su base volontaria, sostituendolo con un regime obbligatorio. L'EDPB e l'EDPS raccomandano di chiarire che, in tali circostanze, i fornitori di servizi che non saranno obbligati a effettuare tali trattamenti ai sensi della proposta di regolamento non potranno più procedere su base volontaria, a meno che

ciò non sia previsto dalle leggi nazionali ad essi applicabili che recepiscono la Direttiva 2002/58/CE (Direttiva ePrivacy).

L'EDPB e l'EDPS ritengono che le disposizioni della proposta di regolamento relative alle valutazioni dei rischi che i fornitori di servizi devono effettuare non siano sufficientemente dettagliate e precise per soddisfare i requisiti di certezza, chiarezza e prevedibilità necessari qualora si vada a interferire con il godimento dei diritti fondamentali. La criticità riguarderebbe, in particolare, le disposizioni che regolano la procedura per l'emissione di ordini di individuazione, mirata a un fornitore di servizi. Le tecnologie per l'individuazione di CSAM nuove o sconosciute, rispetto a quelle note, hanno tassi di errore significativamente più elevati e il loro utilizzo potrebbe quindi avere un impatto sproporzionato sui diritti fondamentali (a causa dei falsi positivi).

Viene inoltre rilevato che il regime che si applicherà agli ordini di rilevamento potrebbe indurre i fornitori di servizi soggetti alla proposta di regolamento, a smettere di utilizzare la crittografia end-to-end o a ridurre in altro modo l'efficacia dei loro accordi di crittografia; ciò sarebbe dovuto alla possibilità di dover, da parte di un fornitore dei servizi di specie, ottemperare, in un breve lasso di tempo, ad un ordine di rilevamento da parte di una autorità giudiziaria/amministrativa competente, pena l'applicazione di una sanzione. Su questa base, i due enti si oppongono all'inclusione nella proposta di regolamento di qualsiasi misura che possa, anche indirettamente, indebolire le pratiche di crittografia.

L'EDPB e l'EDPS, peraltro, sono particolarmente critici nei confronti della disciplina della proposta di regolamento che prevede la scansione delle comunicazioni audio al fine di individuare l'adescamento di minori (cosa non consentita dal regolamento 2021/1232). Nel parere osservano che ciò richiederebbe un'intercettazione continua e in diretta, particolarmente invasiva. Hanno inoltre espresso scetticismo nei confronti dell'uso proposto di misure di verifica dell'età per identificare gli utenti minorenni dei servizi, in quanto riconoscono che attualmente non esiste una soluzione tecnologica in grado di valutare l'età con certezza, con il risultato che il fornitore di servizi potrebbe essere incentivato a escludere dall'accesso ai servizi gli adulti dall'aspetto giovanile, oppure a impiegare misure di verifica eccessivamente molto intrusive.

In conclusione, l'EDPB e l'EDPS evidenziano come la proposta di regolamento sollevi serie preoccupazioni in materia di protezione dei dati personali e invitano il legislatore dell'UE a modificarlo per colmare le lacune individuate nel parere, in particolare per quanto riguarda il rispetto dei criteri di necessità e proporzionalità. Nell'attesa che venga adottato il nuovo provvedimento, anche alla luce delle modifiche proposte dall'EDPB e dall'EDPS, i fornitori i cui servizi possono essere utilizzati per condividere abusi sessuali su minori online o per adescare minori online, potranno continuare a cercare di affrontare tali attività su base volontaria ai sensi del regolamento 2021/1232.

FRANCESCO GROSSI

[https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-042022-proposal\\_en](https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en)

## **NOYB denuncia Google alla CNIL per l'invio di e-mail pubblicitarie non richieste senza consenso degli utenti.**

Il 24 agosto 2022 l'organizzazione non governativa NOYB – *European Center for Digital Rights* (NOYB) ha presentato davanti all'Autorità francese per la protezione dei dati (*Commission nationale de l'informatique et des libertés*, nel prosieguo “**CNIL**”) una denuncia contro Google per l'invio di e-mail pubblicitarie non richieste – senza un valido consenso degli utenti – attraverso la piattaforma di posta elettronica Gmail.

Google, infatti, invia agli utenti Gmail messaggi pubblicitari che compaiono direttamente nella loro casella di posta come normali e-mail. Trattandosi di comunicazioni aventi contenuto promozionale, queste rientrano nella categoria del marketing diretto e, come tali, sono soggette all'applicazione della Direttiva 2002/58/CE (“**Direttiva ePrivacy**”), secondo cui l'invio di materiale pubblicitario o di comunicazioni commerciali è consentito solo previo un valido consenso espresso dell'utente destinatario. Tuttavia, mentre per i messaggi di posta indesiderata (c.d. *spam*) Gmail opera automaticamente un filtro spostando le e-mail direttamente in una cartella separata, i messaggi promozionali non richiesti di Google vengono inviati direttamente alla casella di posta dell'utente senza che sia applicato alcun filtro.

Sul tema si era pronunciata anche la Corte di Giustizia dell'Unione Europea con la sentenza del 25 novembre 2021, *StWL Städtische Werke Lauf a.d Pegnitz* (C-102/20) in cui affermava che la visualizzazione nella casella e-mail in arrivo di messaggi pubblicitari in una forma simile a quella di un vero e proprio messaggio di posta elettronica (c.d. *inbox advertising*) costituisce un uso della posta elettronica a fini di commercializzazione diretta ai sensi della Direttiva ePrivacy. Secondo quella sentenza, tali messaggi presentano un elevato rischio di confusione per l'utente che può essere indotto a cliccare sulla stringa corrispondente al messaggio pubblicitario ed essere così reindirizzato al sito Internet contenente la relativa pubblicità senza aver prestato alcun consenso. I messaggi di *inbox advertising*, infatti, si distinguono visivamente dall'elenco degli altri messaggi di posta elettronica solo per il fatto che la data è sostituita dalla dicitura “Annuncio” e non è menzionato alcun mittente.

Nonostante la citata pronuncia della Corte europea, Google ha continuato ad utilizzare lo strumento dell'*inbox advertising* senza il consenso degli utenti, violando così la normativa applicabile. Per questo motivo NOYB ha presentato la denuncia all'autorità francese che potrà decidere direttamente, senza dover consultare autorità di controllo di altri Paesi UE. Trattandosi infatti di una violazione della Direttiva ePrivacy e non del Regolamento UE 2016/679 (“**GDPR**”) non opera il meccanismo di cooperazione previsto dall'art. 60 GDPR.

CHIARA RAUCCIO

<https://noyb.eu/it/gmail-crea-email-di-spam-nonostante-la-sentenza-della-cgue>

2022/3(9)CR

### **Il Garante privacy esprime parere negativo sullo schema di decreto sull'Ecosistema Dati Sanitari.**

Il 22 agosto 2022 l'autorità Garante per la protezione dei dati personali (“**Garante privacy**” o “**Garante**”) ha emesso un parere negativo sullo schema di decreto presentato dal Ministero della salute e dal Ministero per l'innovazione tecnologica e la transizione digitale che prevede la realizzazione del c.d. Ecosistema Dati Sanitari (“**EDS**”). L'istituzione dell'EDS, prevista dall'art. 12, comma 15-quater del d.l. n. 179/2012 con l'obiettivo di “garantire il coordinamento informatico e assicurare servizi omogenei sul territorio nazionale”, si inserisce nell'ambito della riforma del Fascicolo sanitario elettronico (“**FSE**”). Per tale motivo il Garante si è pronunciato parallelamente – chiedendo alcune modifiche – anche sullo schema di decreto sul FSE che risulta preliminare a quello sull'EDS.

Il Garante privacy ha precisato di condividere l'esigenza di introdurre strumenti che agevolino lo sviluppo di servizi sanitari digitali; tuttavia, ha sottolineato come questo non possa avvenire a discapito dei diritti fondamentali dei cittadini, il cui rispetto deve sempre essere tenuto nella massima considerazione. Questo risulta particolarmente vero nel caso in esame in quanto lo schema di decreto prevede la costituzione di quella che il Garante ha definito la “più grande banca dati sulla salute del nostro Paese”. L'EDS, infatti, comporterebbe la duplicazione di dati e documenti sanitari già presenti nel FSE dando luogo a un database che raccoglierebbe a livello centralizzato, senza garanzie di anonimato per gli assistiti, dati e documenti sanitari relativi a tutte le prestazioni sanitarie erogate sul territorio nazionale. Considerata la quantità e la delicatezza dei dati trattati, nonché la presenza di un trattamento sistematico su larga scala anche attraverso logiche algoritmiche, si rende necessaria una regolamentazione che garantisca il pieno rispetto dei principi generali del Regolamento UE 2016/679 (“**GDPR**”). Al contrario, il Garante ha ravvisato una serie di violazioni della disciplina in materia di protezione dei dati personali che lo hanno portato ad esprimere un parere negativo sullo schema di decreto, indicando ai Ministeri competenti le misure necessarie per superare le criticità riscontrate.

In particolare, il Garante ha osservato come lo schema di decreto non adempia alla funzione ad esso assegnata dall'art. 12, comma 15-quater del d.l. 179/2012 – delineare “i contenuti dell'EDS, le modalità di alimentazione dell'EDS, nonché i soggetti che hanno accesso all'EDS, le operazioni eseguibili e le misure di sicurezza per assicurare i diritti degli interessati” – in quanto non disciplina specificamente tali aspetti, ma si limita a delineare un quadro generale rinviando la disciplina di dettaglio a una serie di successivi decreti non ancora emanati. In questo modo il decreto risulta una “scatola vuota” dal contenuto indeterminato che rende impossibile all'autorità una effettiva valutazione della correttezza e adeguatezza dei trattamenti, in particolare con riferimento ai principi di proporzionalità e minimizzazione dei dati.

Anche sui diritti degli interessati, lo schema di decreto rinvia sommariamente ai diritti esercitabili con riferimento al trattamento effettuato attraverso il FSE. Tuttavia, come sottolinea il Garante, i trattamenti effettuati mediante il FSE e quelli effettuati in relazione all'EDS presentano numerose differenze sotto il profilo delle finalità perseguite e della relativa titolarità. Pertanto, il rinvio non permette di chiarire alcuni temi quali le modalità e le conseguenze dell'esercizio del diritto di oscuramento e di revoca del consenso.

Ulteriori criticità sono date dall'estrema genericità nell'indicazione dei servizi resi dall'EDS, nonché dalla mancata previsione di livelli diversificati di accesso a tali servizi e dalla

scarsa chiarezza sui ruoli privacy assunti dai diversi soggetti coinvolti nelle fasi di raccolta ed elaborazione dei dati.

Infine, il Garante ha riscontrato numerose imprecisioni e carenze (in particolare nell'individuazione dei rischi per gli interessati) nella valutazione d'impatto svolta ai sensi dell'art. 35 GDPR dal Ministero della salute e fornita all'autorità ancora in versione "bozza". Anche in questo caso il Garante ha fornito indicazioni sulle necessarie modifiche e integrazioni del documento invitando il Ministero a coinvolgere nella valutazione del rischio anche strutture con competenze mediche ed etiche.

A seguito del parere in esame, lo schema di decreto torna nelle mani dei Ministeri competenti che dovranno quanto prima provvedere a riformularlo alla luce delle considerazioni del Garante al fine di ottenere il parere positivo dello stesso per procedere alla creazione dell'EDS.

CHIARA RAUCCIO

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9802752>

2022/3(10)LC

### **Accesso ai risultati della ricerca scientifica finanziata con fondi federali: nuove linee guida negli Stati Uniti.**

In data 25 agosto 2022, l'*Office of Science and Technology Policy* (OSTP) del governo federale degli Stati Uniti ha pubblicato le nuove linee guida per garantire un accesso equo, immediato e libero ai risultati della ricerca scientifica finanziata dal governo federale con fondi pubblici ("*Memorandum OSTP 2022*"). L'obiettivo dichiarato del governo americano è quello di garantire le stesse opportunità non solo di accesso ai risultati della ricerca, ma anche di partecipazione attiva di tutta la comunità americana al progresso scientifico del Paese, contrastando quelle che a tutt'oggi rappresentano forme di discriminazione all'accesso alla scienza e, più in generale, alla cultura.

In questa prospettiva, la Casa Bianca ha stabilito che tutte le ricerche finanziate dalle agenzie federali (ovvero l'equivalente dei nostri Ministeri) debbano essere pubblicate in modo tale che siano immediatamente e gratuitamente consultabili dal pubblico.

Un precedente intervento in questa direzione risale al 2013 (cd. *Memorandum OSTP 2013*) ed ha rappresentato un punto di svolta senza precedenti, giacché in grado di innescare movimenti sociali per il libero accesso alla ricerca che, di lì a poco, si sarebbero diffusi in tutti i singoli Stati americani ed anche oltre i confini degli stessi. Negli anni successivi, le stesse agenzie federali soggette al *Memorandum OSTP 2013* hanno sviluppato piani e attuato politiche in coerenza con le indicazioni ricevute dal governo.

Nel *Memorandum OSTP 2022* vengono fornite nuove linee guida alle agenzie per l'aggiornamento delle politiche di accesso aperto. In particolare, l'OSTP raccomanda di:

- aggiornare le proprie politiche di accesso pubblico non oltre il 31 dicembre 2025, al fine di rendere accessibili le pubblicazioni e i dati, eliminando l'attuale embargo di un anno, così da renderli gratuiti e accessibili a tutti;
- stabilire procedure che garantiscano la trasparenza e l'integrità della ricerca scientifica nelle politiche di accesso;

- coordinarsi con l'OSTP per garantire un'equa distribuzione dei risultati e dei dati della ricerca finanziati a livello federale.

Le principali novità introdotte con questo intervento sono dunque:

*i) eliminazione dell'embargo di 12 mesi per gli articoli scientifici peer-reviewed finanziati dal governo federale:* prima di questa previsione, l'accesso ai risultati della ricerca finanziata a livello federale era a pagamento o limitato solo a coloro che avevano accesso attraverso biblioteche o altre istituzioni; ora, mezzi finanziari e accesso privilegiato non devono più costituire un prerequisito per accedere ai benefici della ricerca finanziata dal governo federale e, quindi, dai contribuenti americani;

*ii) rafforzamento dei piani di condivisione dei dati rispetto al Memorandum 2013, rendendoli immediatamente disponibili al momento della pubblicazione:* fornire i dati a supporto di nuovi articoli scientifici migliora la trasparenza e la possibilità di basarsi sui risultati delle ricerche precedenti. L'accesso del pubblico ai dati di ricerca finanziati dal governo federale aiuta anche a "livellare" il terreno su cui misurarsi, in un panorama di finanziamenti altamente diseguale tra le diverse discipline e comunità accademiche, offrendo così la possibilità a studiosi, discenti e in più in generale al pubblico, un uso secondario dei dati, altrimenti indisponibili. Le nuove linee guida chiariscono, inoltre, che la condivisione dei dati deve avvenire in modo responsabile e alle stesse agenzie è richiesto di garantire la protezione del diritto alla *privacy* e alla sicurezza nella circolazione dei dati.

Tuttavia, garantire che tutti i cittadini americani possano beneficiare in modo equo e libero di questo importante mutamento nelle politiche di *open access* richiede tempo, impegno e collaborazione da parte di tutte le agenzie e dei soggetti a vario titolo coinvolti. In tal senso, l'*Office of Science and Technology Policy* ha annunciato il ricorso a diverse risorse per supportare questo cambiamento.

Attraverso una nuova sottocommissione del *National Science and Technology Council on Open Science* (SOS), l'OSTP sta conducendo un processo di coordinamento per garantire che le politiche di accesso pubblico siano accompagnate e sostenute in maniera graduale, soprattutto per le componenti più vulnerabili dell'ecosistema della ricerca, incapaci di sostenere i costi crescenti associati alla pubblicazione di articoli ad accesso aperto, come i ricercatori in fase iniziale o di istituzioni al servizio delle minoranze. Le nuove linee guida, inoltre, consentono ai ricercatori di includere nelle loro proposte di *budget* di finanziamento alla ricerca i costi di pubblicazione e condivisione dei dati.

Si sottolinea, altresì, la necessità di combattere le disuguaglianze esistenti nella distribuzione dei finanziamenti: molte agenzie federali, tra cui il Dipartimento dell'Energia, il *National Institutes of Health* e la *National Science Foundation*, hanno lanciato programmi volti a concedere sovvenzioni a sostegno della fase iniziale delle carriere dei ricercatori, azzerando ogni forma di discriminazione basata sulla razza e sul genere. L'OSTP ha anche pubblicato il report *Economic Landscape of Federal Public Access Policy* per aiutare a comprendere meglio i potenziali impatti economici di questi cambiamenti politici su tutta la popolazione.

LUCIO CASALINI

<https://www.whitehouse.gov/wp-content/uploads/2022/08/08-2022-OSTP-Public-Access-Memo.pdf>

## **Le proposte normative dell'11 ottobre 2022 del Financial Stability Board in materia di cripto-attività e global stablecoins.**

L'11 ottobre 2022 il *Financial Stability Board* (“**FSB**”) ha avviato una consultazione sulla proposta per una regolamentazione internazionale delle cripto-attività. La proposta consta di due documenti principali: (i) raccomandazioni per un quadro regolamentare e di vigilanza dei servizi e mercati in cripto-attività (anche, “**raccomandazioni**”); (ii) revisione delle raccomandazioni per la regolamentazione e la vigilanza dei c.d. *global stablecoins* (“**GSCs**”) *arrangements* (anche, “**revisione**”). La consultazione avrà termine a dicembre 2022.

Quanto alle raccomandazioni per un quadro regolamentare delle cripto-attività, a partire da un'analisi del mercato attuale e delle iniziative regolamentari intraprese, il FSB riconosce come sia necessario promuovere degli approcci di regolamentazione e vigilanza che siano completi e tra loro coerenti, dati i rischi che ne potrebbero derivare per la stabilità finanziaria a livello globale. Ne segue che le raccomandazioni delineate dovrebbero applicarsi a tutte le cripto-attività e giurisdizioni.

In generale, le autorità dovrebbero disporre di adeguati poteri e strumenti per la regolamentazione e supervisione dei servizi e mercati in cripto-attività (*Recommendation 1*), nonché predisporre un quadro normativo che vada a disciplinare sia gli emittenti che i prestatori di servizi (*Recommendation 2*). In particolare, tale quadro normativo dovrebbe ispirarsi al principio “*same activity, same risk, same regulation*” e, quindi, guardare non alla forma, ma bensì alla funzione economica svolta dalla cripto-attività o dall'operatore di mercato considerato.

Il FSB sottolinea anche come le cripto-attività abbiano natura *cross-border* e come, dunque, ciascun approccio regolamentare e di supervisione dovrebbe prevedere cooperazione e coordinamento tra le diverse autorità, sia a livello domestico che internazionale (*Recommendation 3*).

Nel documento di consultazione si evidenzia poi come un eventuale quadro regolamentare dovrebbe affrontare specifici rischi e aspetti delle cripto-attività. In particolare, il focus ricade sulle attività di *risk management* e di *data management*, nonché sulla *governance* delle iniziative di cripto-attività. In particolare, secondo la proposta, gli emittenti e prestatori di servizi in cripto-attività dovrebbero predisporre una struttura di governo societario trasparente che identifichi chiaramente le responsabilità e i ruoli degli attori coinvolti (*Recommendation 4*), nonché un *framework* adeguato per la raccolta e gestione dei dati e per la *disclosure* di informazioni rilevanti (*Recommendation 6* e *Recommendation 7*). In aggiunta, i prestatori di servizi in cripto-attività dovrebbero dotarsi di robusti sistemi di gestione del rischio, con particolare attenzione ai rischi per la stabilità finanziaria (*Recommendation 5*).

Da ultimo, si sottolinea come le autorità dovrebbero identificare e monitorare le interconnessioni - sia nello stesso ecosistema delle cripto-attività che con il sistema finanziario tradizionale - che potrebbero sfociare in rischi per la stabilità finanziaria (*Recommendation 8*) e contenere quei rischi che potrebbero derivare dall'esercizio congiunto di più funzioni e attività in capo a uno stesso soggetto (*Recommendation 9*). In particolare, quanto all'ultimo punto, il focus dovrebbe ricadere su quei prestatori di servizi in cripto-attività verticalmente integrati, quali, ad esempio, le piattaforme di scambio di cripto-attività.

Quanto alle raccomandazioni per la regolamentazione e supervisione dei GSCs, la proposta consiste in una revisione delle *High-Level Recommendations* già definite nel 2020. Sebbene l'obiettivo rimanga quello di promuovere approcci regolatori coerenti ed efficaci, ciò che cambia è l'ambito di applicazione. Nonostante la dimensione del mercato sia ancora

contenuta e limitata all'ecosistema delle cripto-attività, il FSB riconosce come i GSCs potrebbero rapidamente crescere in rilevanza e diffusione. Sicché, nel delineare un quadro normativo, sarebbe necessario non solo considerare i GSCs, ma anche quegli *stablecoins* potenzialmente capaci di diventare GSCs in un futuro prossimo. In ogni caso, si sottolinea come tali *stablecoins* dovrebbero comunque essere sempre soggetti alle raccomandazioni definite per le cripto-attività in generale.

Dopodiché, nella revisione si enfatizza come le autorità dovrebbero essere pronte a contenere i rischi per la stabilità finanziaria che potrebbero derivare dai GSCs (*High-level Recommendation 1*) ed esercitare un controllo completo su quelle che sono le attività e funzioni dei GSCs (*High-level Recommendation 2*). Particolare attenzione dovrebbe essere posta dalle autorità ai *wallet service providers* e alle *trading platforms*, data la criticità di tali servizi per la stabilizzazione del valore e custodia dei GSCs.

La revisione ha poi ad oggetto il rafforzamento di alcuni punti circa aspetti critici dei GSCs, quali, ad esempio, la struttura di governo societario o sistemi di gestione del rischio. In particolare, la revisione mira a rendere chiaro come la struttura di governo societario dei GSCs debba essere definita in modo trasparente e in maniera tale da non impedire l'applicabilità della regolamentazione e degli *standard* vigenti (*High-level Recommendation 4*). Nei sistemi di gestione del rischio, invece, particolare attenzione dovrebbe essere posta alle misure in materia di riciclaggio di denaro e finanziamento del terrorismo, nonché ad aspetti di *liquidity risk management* da attivare nel caso di fenomeni di *run* (*High-level Recommendation 5*).

In merito alla gestione e raccolta di dati, la revisione propone di dare potere all'Autorità di accedere ai dati rilevanti quando necessario per fini regolamentari, a prescindere da dove questi siano localizzati (*High-level Recommendation 6*).

Particolare attenzione viene poi riservata a quegli elementi che contribuiscono alla stabilizzazione del valore dei GSCs. In particolare, oltre a obblighi informativi generali, la revisione prevede la *disclosure* dei *reserve assets* e dei dettagli del processo e dei diritti di rimborso degli utenti (*High-level Recommendation 8*). Ciò nella misura in cui l'emittente non sia già soggetto a requisiti informativi analoghi sotto altri *framework* regolamentari. Sempre in merito alla stabilizzazione del valore, la revisione si focalizza anche sulla redimibilità dei GSCs, prevedendo che tutti gli utenti debbano avere un chiaro diritto di rimborso nei confronti dell'emittente o dei *reserve assets* (*High-level Recommendation 9*). In aggiunta, per assicurare la stabilizzazione del valore ed evitare fenomeni di panico, le autorità dovrebbero richiedere ai GSCs di dotarsi di meccanismi di stabilizzazione efficaci, procedure di rimborso chiare e rispettare i requisiti prudenziali di capitale e liquidità.

Da ultimo, la revisione prevede come i GSCs dovrebbero essere conformi a ogni requisito regolamentare, sia specifico che generale, applicabile già prima dell'avvio delle operazioni (*High-level Recommendation 10*).

Alice Filippetta

<https://www.fsb.org/2022/10/regulation-supervision-and-oversight-of-crypto-asset-activities-and-markets-consultative-report/>

<https://www.fsb.org/2022/10/review-of-the-fsb-high-level-recommendations-of-the-regulation-supervision-and-oversight-of-global-stablecoin-arrangements-consultative-report/>

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

Il 27 ottobre 2022 è stato pubblicato nella Gazzetta ufficiale dell’Unione Europea il Regolamento (UE) 2022/2065 “relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)”, noto come *Digital Services Act* (DSA) (di seguito anche solo il “**Regolamento**”). Il Regolamento rappresenta l’ultima tappa di un percorso avviato nel dicembre 2020 dalla Commissione europea con la proposta da COM(2020) 825 final (su cui v. la notizia [2021/1\(3\)ST](#)).

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

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

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

di servizi intermediari, qualora le stesse perseguano legittimi obiettivi di interesse pubblico diversi da quelli del Regolamento.

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

Rispetto alla proposta di regolamento di dicembre 2020, sono interessanti alcuni chiarimenti su cosa debba intendersi per conoscenza o consapevolezza effettiva di contenuti e attività illegali. Il Considerando 22) del Regolamento esplicita che tale conoscenza o consapevolezza effettiva non può essere considerata acquisita per il solo motivo che il prestatore sia consapevole, in senso generale, del fatto che il suo servizio è utilizzato anche per memorizzare contenuti illegali. Inoltre, la circostanza che il prestatore proceda a un'indicizzazione automatizzata delle informazioni, oppure utilizzi una funzione di ricerca basata sul profilo o sulle preferenze dei destinatari del servizio, non è un motivo sufficiente per considerare che il prestatore abbia una conoscenza «specifica» di attività illegali realizzate sulla medesima piattaforma o di contenuti illegali ivi memorizzati.

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

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

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

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

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

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

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

Il dato è ribadito nella formulazione del nuovo articolo 25 del Regolamento, ai sensi del quale i fornitori di piattaforme *online* non progettano, organizzano o gestiscono le loro interfacce *online* in modo tale da ingannare o manipolare i destinatari dei loro servizi o da materialmente falsare o compromettere altrimenti la capacità dei destinatari dei loro servizi di prendere decisioni libere e informate.

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

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

Ulteriore novità importante, che merita di essere segnalata, è la maggiore attenzione alla protezione *online* dei minori, alla quale è dedicato l'art. 28 del Regolamento. Si richiede, infatti, che i fornitori di piattaforme *online* accessibili ai minori adottino misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori. Sono previsti specifici divieti anche con riferimento alla pubblicità basata sulla profilazione, qualora i fornitori di piattaforme siano consapevoli, con ragionevole certezza, che il destinatario del servizio sia un minore.

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

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

Restano due aspetti che meritano di essere segnalati come novità del Regolamento (UE) 2022/2065 rispetto alla proposta di COM(2020) 825 final. Il primo riguarda la valutazione del rischio di cui all'art. 34, che corrisponde all'art 26 di COM(2020) 825 final, dal quale si

differenza nel par.1, per i riferimenti alla diligenza nella valutazione dei rischi sistemici, alla possibilità che tali rischi possano derivare da sistemi algoritmici, alla previsione che la valutazione del rischio debba essere specifica per i loro servizi e proporzionata ai rischi sistemici, tenendo in considerazione la loro gravità e la loro probabilità.

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

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

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

SARA TOMMASI

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

2022/4(2)VR

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

Il 14 settembre 2022, dopo meno di due anni dalla proposta della Commissione europea COM(2020) 842 final del 15 dicembre 2020 (di seguito la "**Proposta**": su cui v. la notizia [2021/1\(4\)EMI](#)), è intervenuta l'approvazione del Regolamento 2022/1925/UE del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive 2019/1937/UE e 2020/1828/UE (c.d. *Digital Markets Act* o regolamento sui mercati digitali, di seguito "**DMA**" o il "**Regolamento**").

Perno della strategia digitale dell'Unione Europea (*Shaping Europe's Digital Future*: [249](https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-</a></p></div><div data-bbox=)

digital-future-feb2020\_en\_4.pdf), il DMA appronta una disciplina dei mercati digitali ponendo enfasi sui servizi di piattaforma di base forniti dai cc.dd. *gatekeepers* (controllori dell'accesso).

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

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

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

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

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

terzo requisito può presumersi se le soglie di cui alla lettera *b*) sono state raggiunte in ciascuno degli ultimi tre esercizi finanziari.

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

Ciò posto, è opportuno porre l'accento su un aspetto fortemente indicativo della linea di politica del diritto seguita dal DMA. Il legislatore europeo si è premurato in più punti di prevedere salvaguardie avverso la possibile obsolescenza delle prescrizioni a causa del mutamento tecnologico e delle dinamiche di mercato. Sebbene si tratti di un regolamento, e debba parlarsi perciò di uniformazione, con relativa assunzione del monopolio disciplinare in materia, il quadro si pone come *level playing field* e, dunque, come statuto di base suscettibile di (auto)integrazione. In quest'ottica, entrambe le fondamentali nozioni di *gatekeeper* e di servizi di piattaforma di base possono essere ampliate dalla Commissione ai sensi, rispettivamente, degli artt. 17 e 19 DMA, previo esperimento di una pertinente indagine di mercato (art. 16 DMA).

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

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

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

Come sopra accennato, alla rapida evoluzione tecnologica e dei mercati il legislatore europeo risponde, oltre che – s'intende – con l'ecchegiata premura per la proporzionalità delle misure, soprattutto con una regolazione programmaticamente flessibile. In quest'ottica,

ai sensi dell'art. 12 DMA, la Commissione, mediante l'agile strumento della legislazione delegata, può aggiornare gli obblighi di cui agli artt. 5 e 6 DMA, con i limiti di cui al par. 2 dell'art. 12 DMA. Come evidenziato al Considerando 69 DMA, le integrazioni sono da adottare esclusivamente a valle di indagini approfondite e capillari sulla natura e sull'impatto di pratiche specifiche sul mercato, per sondare adeguatamente la slealtà e la portata limitativa della contendibilità.

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

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

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

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

VALENTINO RAVAGNANI

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

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

Nella Gazzetta ufficiale dell’Unione europea del 27.12.2022 è stato pubblicato il Regolamento (UE) 2022/2554 del 14.12.2022 relativo alla resilienza operativa digitale per il settore finanziario (di seguito solo il “**Regolamento**” o “**DORA**”, acronimo per *Digital Operational Resilience Act*). Si tratta del testo rispondente al documento P9\_TA(2022)0381 del 10 novembre 2022 con il quale il Parlamento europeo approvava, con alcune modifiche frutto di un compromesso col Consiglio, la proposta di regolamento COM(2020)0595.

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

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

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

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

L’art. 3 del Regolamento elenca una serie di definizioni, mentre il successivo art. 4 richiama il principio di proporzionalità, sancito anche nel considerando 13, per cui le norme del DORA dovranno essere applicate “*tenendo conto delle ... dimensioni e del ... profilo di rischio*”

*complessivo, nonché della natura, della portata e della complessità dei loro servizi, delle loro attività e della loro operatività”.*

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

### **I. Governance e organizzazione (art. 5 DORA)**

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

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

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

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

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

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

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

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

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

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

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

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

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

Il Regolamento, inoltre, all’art. 18, par. 2 stabilisce che le minacce informatiche si definiscono significative “*in base alla criticità dei servizi a rischio, comprese le operazioni dell’entità finanziaria, il numero e/o la rilevanza di clienti o controparti finanziarie interessati e l’estensione geografica delle aree a rischio*”. Se, da un lato, la registrazione di tali minacce è obbligatoria, dall’altro, il DORA, coerentemente con quanto stabilito dalla direttiva 2016/1148/UE (c.d. direttiva NIS), prevede che la notifica alle Autorità nazionali di vigilanza sia volontaria laddove le entità finanziarie “*ritengano che la minaccia sia rilevante per il sistema finanziario, gli utenti dei servizi o i clienti*” (art. 19).

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

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

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

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

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

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

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

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

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

EMANUELE STABILE

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

2022/4(4)SO

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

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

La prima integrazione riguarda la nozione di dipendenza economica. Come noto, la dipendenza economica non è di per sé vietata dalla l. subfornitura, essendone invece vietato l'abuso. Interessante appare la formulazione della norma che richiede di guardare agli “effetti di rete” e alla “disponibilità dei dati” per stabilire se possa dirsi che una piattaforma digitale abbia o meno un “ruolo determinante per raggiungere utenti finali o fornitori” dell'impresa di cui importi predicare una situazione di dipendenza economica dalla medesima piattaforma digitale. La seconda integrazione riguarda per l'appunto l'abuso di dipendenza economica. La norma prevede come figure sintomatiche di abuso di dipendenza economica pratiche informative ingannevoli (commissive od omissive) relativamente al servizio erogato dalla piattaforma digitale, oppure pratiche della piattaforma digitale che consistono nel pretendere dall'impresa prestazioni ingiustificate ovvero nell'ostacolare il ricorso da parte di quest'ultima a fornitori diversi. Con la terza modifica è stata disposta la competenza delle sezioni specializzate in materia di impresa per le controversie di abuso di dipendenza economica ai sensi della l. subfornitura. È una modifica di cui si avvertiva l'esigenza da tempo, a prescindere dai rapporti concernenti le piattaforme digitali.

In particolare:

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

- al terzo comma dell'art. 9 l. subfornitura è stato aggiunto, in fine, il seguente periodo:  
«Le azioni civili esperibili a norma del presente articolo sono proposte di fronte alle sezioni specializzate in materia di impresa di cui all'articolo 1 del decreto legislativo 27 giugno 2003, n. 16»

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

SALVATORE ORLANDO

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

2022/4(5)RA

### **La EU Interinstitutional declaration on digital rights and principles del 14.11.2022**

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

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

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

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

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

Il primo capitolo della Dichiarazione – finalizzato, come detto, a “*mettere le persone al centro della trasformazione digitale*” ponendo la tecnologia “*al servizio [...] e a beneficio di tutti gli europei*”

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

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

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

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

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

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

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

RICCARDO ALFONSI

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

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

2022/4(6)DI

## **Il codice deontologico “rafforzato” del 2022 di buone pratiche contro la disinformazione.**

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

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

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

Per quanto concerne l’oggetto, il codice rafforzato fa riferimento alla disinformazione come definita dalla Commissione europea nella Comunicazione sull’*European Democracy Action Plan* del 3 dicembre 2020, COM(2020) 790 final (su cui v. la notizia [2021/1\(1\)DPDM](#)), ripetendone le varie accezioni di cattiva informazione (“contenuti falsi o fuorvianti, condivisi senza intenzione fraudolenta, anche se gli effetti possono comunque essere dannosi, ad esempio quando le persone condividono informazioni false con amici e familiari in buona fede”), disinformazione (“contenuto falso o fuorviante, diffuso con l’intento di ingannare o

ottenere un guadagno economico e che può provocare danni pubblici”), influenza delle informazioni (“sforzi coordinati da parte di soggetti nazionali o esterni volti a influenzare il pubblico destinatario utilizzando una serie di mezzi ingannevoli, tra cui la soppressione di fonti di informazione indipendenti in combinazione con la disinformazione”) e di ingerenze straniere nello spazio informativo (“misure coercitive e ingannevoli impiegate da un soggetto statale straniero o dai suoi agenti per ostacolare la libertà di informazione e di espressione della volontà politica degli individui”).

Il codice rafforzato si compone di un preambolo e di sette sezioni, in cui si affermano 44 impegni (*commitment*). Rispetto a molti di questi impegni assunti dai firmatari, il codice prevede anche delle pratiche attuative (*measures*) ed offre indicazioni concrete. La sezione sul controllo delle inserzioni pubblicitarie (“*scrutiny of ad placements*”) racchiude impegni importanti come quello a evitare l'uso di sistemi pubblicitari per diffondere, sotto forma di messaggi pubblicitari, della disinformazione. La sezione successiva si occupa del tema dei messaggi pubblicitari politici e riflette le osservazioni che la Commissione e gli stessi firmatari hanno ricavato dall'osservazione delle ultime elezioni europee. È interessante notare che il codice rafforzato non offre una specifica definizione di *political advertising*, preferendo richiamare quella contenuta nella proposta di regolamento relativo alla trasparenza e al targeting della pubblicità politica (art. 2.1, 2: “la preparazione, collocazione, promozione, pubblicazione o diffusione, con qualsiasi mezzo, di un messaggio: a) di, a favore o per conto di un attore politico, salvo se di natura meramente privata o meramente commerciale; oppure b) che possa influenzare l'esito di un'elezione o di un referendum, di un processo legislativo o regolamentare o di un comportamento di voto”) (su questa proposta v. la notizia [2022/1\(6\)SO](#)). Non dovesse tale proposta di regolamento sulla pubblicità politica essere approvata nel primo anno di vigenza del codice rafforzato, i firmatari del codice rafforzato si impegnano ad affidare a una task-force l'elaborazione di una definizione analoga. La sezione sull'integrità dei servizi contiene tre raccomandazioni, tra cui quella propria dei fornitori di sistemi di intelligenza artificiale e che diffondono contenuti generati e manipolati dall'IA attraverso i loro servizi (es. *deepfakes*) a prendere in considerazione gli obblighi di trasparenza e l'elenco delle pratiche manipolative di cui alla proposta di regolamento sull'intelligenza artificiale (su cui v. la notizia [2021/1\(1\)DPDM](#)). La sezione “*empowering users*” presenta numerosi impegni, tra cui quello a ridurre al minimo i rischi di propagazione virale di contenuti di disinformazione tramite l'adozione di pratiche di progettazione sicure nello sviluppo. La sezione “*empowering the research community*” disciplina, tra le altre cose, l'accesso automatizzato (es. API) e l'utilizzo per finalità di ricerca dei dati non personali, anonimizzati, aggregati o già pubblici. Un significativo impegno a dialogare e coinvolgere specifici soggetti è previsto nella sezione “*Empowering the fact-checking community*”; qui, ad esempio al *commitment* 31, si afferma l'impegno a integrare, mettere in mostra o comunque utilizzare in modo coerente il lavoro dei *fact-checkers* nei servizi offerti dalle varie piattaforme che hanno sottoscritto il codice rafforzato. Le sezioni finali contengono impegni relativi alla trasparenza circa l'implementazione del codice rafforzato, all'istituzione di una task-force *ad hoc* e al continuo monitoraggio dello stesso codice, in vista di un suo futuro aggiornamento. Tra i firmatari figurano [Adobe](#), [Associazione europea delle agenzie di comunicazione \(EACA\)](#), [Google](#), [IAB Europe \(Interactive Advertising Bureau Europe\)](#), [Meta](#), [Microsoft](#), [Reporter senza frontiere \(RSF\)](#), [TikTok](#), [Twitch](#), [Twitter](#), [Vimeo](#) e [Federazione mondiale degli inserzionisti \(WFA\)](#). Ciascuno di essi ha firmato gli impegni in un documento, pubblicamente accessibile, che prevede le misure pertinenti per i propri servizi.

DANIELE IMBRUGLIA

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

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

2022/4(7)ST

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

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

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

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

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

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

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

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

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

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

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

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

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

Il Tribunale distrettuale, sposando di fatto le ragioni delle grandi piattaforme, considera incostituzionale la Sezione 2 del *Texas House Bill 20* per diverse ragioni. Prima di tutto, ritiene che siano imposti alle piattaforme obblighi considerati eccessivamente gravosi in ragione dell'elevato numero di messaggi che transitano sui siti *web*. Inoltre, il Tribunale afferma che le «*social media platforms are not common carriers*» e che la gestione e organizzazione dei contenuti rientri nella discrezionalità editoriale delle piattaforme. In base a questa impostazione la «*prohibition on viewpoint-based censorship*» violerebbe la discrezionalità editoriale delle piattaforme. Anche quest'ultima, a detta delle piattaforme, sarebbe protetta dal Primo Emendamento. In merito, la *United States Court of Appeals for the Fifth Circuit* dimostra tutto il suo disappunto, evidenziando che è contraddittorio l'atteggiamento delle piattaforme che invocano la discrezionalità editoriale degli editori, pur non volendo assumersi le relative responsabilità. Le piattaforme, infatti, rivendicano il loro ruolo di intermediari di contenuti riferibili ad altri e dalle stesse difficilmente controllabili, anche in ragione del numero elevato di post che consentono di pubblicare. Il dato spiega il ricorso delle piattaforme agli algoritmi per escludere determinati contenuti e la diversità del controllo effettuato rispetto al classico giudizio editoriale tipico dei giornali.

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

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

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

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

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

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

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

SARA TOMMASI

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

2022/4(8)CR

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

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

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

La controversia nasceva dal fatto che, a seguito di un guasto tecnico che aveva interessato il funzionamento di un server, la Digi aveva creato una banca dati di test in cui aveva copiato

i dati personali di circa un terzo dei clienti abbonati alla sua newsletter, dati che erano stati originariamente raccolti ai fini della conclusione e dell'esecuzione dei contratti di abbonamento. Successivamente, dopo aver effettuato i test necessari e aver corretto l'errore, la Digi non aveva soppresso la banca dati di test, per cui i dati personali erano rimasti conservati in tale banca dati per quasi 18 mesi, finché la stessa non era stata oggetto di un attacco *hacker*.

La Corte ungherese ha sollevato davanti alla CGUE due questioni: (i) se il principio della limitazione della finalità previsto dall'art. 5, par. 1, lett. *b)* GDPR impedisca la registrazione e la conservazione, in una banca dati creata al fine di effettuare test e di correggere errori, di dati personali precedentemente raccolti e conservati in un'altra banca dati; e (ii) se sia compatibile con il principio della limitazione della conservazione di cui all'art. 5, para. 1, lett. *e)* GDPR il fatto che il titolare del trattamento conservi in un'altra banca dati alcuni dati personali che sono stati raccolti e conservati per una finalità legittima limitata.

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

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

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

CHIARA RAUCCIO

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

**La sentenza CGUE del 27.10.2022 nella causa C-129/21 Proximus (Annuaire électroniques publics) sulle misure da adottarsi da parte del titolare del trattamento di dati personali per informare i motori di ricerca in Internet di una richiesta di cancellazione rivolta agli interessati.**

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

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

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

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

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

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

Su tale questione, la CGUE, facendo riferimento all'articolo 12, paragrafo 2, della direttiva ePrivacy afferma che il consenso dell'abbonato di un operatore di servizi telefonici è necessario affinché i dati personali di tale interessato siano inclusi nei relativi elenchi, pubblicati da fornitori diversi da tale operatore. Il consenso in questione, allo stato attuale e

in assenza di ulteriori e più specifiche indicazioni normative, deve rispettare i requisiti dell'articolo 4, punto 11 del GDPR e può, in ogni caso, essere raccolto da detto operatore o da uno di tali fornitori. Tale consenso, secondo la CGUE si estende a qualsiasi trattamento ulteriore dei dati da parte di imprese terze attive nel mercato dei servizi di consultazione degli elenchi telefonici accessibili al pubblico, sempre che tali trattamenti perseguano lo “stesso scopo” e, dunque, non siano effettuati per finalità non compatibili con quella originaria.

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

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

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

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

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

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

rivolga a uno qualsiasi di essi per avere riconosciuta la sua pretesa anche nei confronti degli altri.

CARMINE ANDREA TROVATO

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

2022/4(10)FDA

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

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

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

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

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

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

FILIPPO D'ANGELO

[https://commission.europa.eu/system/files/2022-11/com2022720\\_0.pdf](https://commission.europa.eu/system/files/2022-11/com2022720_0.pdf)

2022/4(11)SO

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

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

Più precisamente, con un primo comunicato del 18 ottobre 2022, il Garante informava di aver cominciato ad esaminare - alla luce del quadro normativo attuale e al fine di valutare l'adozione di eventuali provvedimenti di sua competenza - recenti iniziative di *paywall* e *cookie wall* poste in essere da una serie di soggetti (non nominati) rispondenti a diverse testate giornalistiche *online*, siti *web* e aziende operanti su Internet nel settore televisivo. Nel comunicato in questione si specificava che le iniziative sottoposte all'esame del Garante riguardavano la messa in campo di sistemi e filtri che condizionano l'accesso ai contenuti alla sottoscrizione di un abbonamento (c.d. *paywall*) o, in alternativa, al rilascio del consenso da parte degli utenti all'installazione di *cookie* e altri strumenti di tracciamento dei dati personali (c.d. *cookie wall*).

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

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

SALVATORE ORLANDO

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

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

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

2022/4(12)VR

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

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

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

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

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

Inoltre, ai sensi dell'Allegato alla l. 3 dicembre 2021, n. 205, di conversione del c.d. Decreto Capienze, d.l. 8 ottobre 2021, n. 139, in assenza di una specifica legge in materia, e comunque fino al 31 dicembre 2023, sono sospesi in Italia l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici, a meno che il trattamento non sia effettuato dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali, previo parere favorevole del Garante privacy reso ai sensi dell'art. 24, co. 1, lett. b) del richiamato d.lgs. n. 51/2018, ovvero dall'autorità giudiziaria nell'esercizio delle funzioni di indagine o di prevenzione e repressione dei reati.

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

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

Il secondo procedimento ha interessato il Comune di Arezzo, che, secondo notizie di stampa, avrebbe intenzione di dar avvio, a partire dal 1° dicembre 2022, alla sperimentazione di "super-occhiali infrarossi". Tali dispositivi, in dotazione agli agenti della Polizia locale, sarebbero in grado di rilevare in tempo reale le infrazioni facenti capo al proprietario del veicolo tramite la lettura del numero di targa delle autovetture. Inoltre, attraverso il

collegamento ad alcune banche dati nazionali, sarebbe possibile verificare la validità dei documenti del guidatore e acquisire alcune informazioni quali, ad esempio, la quantità dei punti residui sulla patente o prescrizioni come l'obbligo di indossare occhiali o lenti a contatto durante la guida.

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

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

VALENTINO RAVAGNANI

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

2022/4(13)ES

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

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

**Il fatto.**

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

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

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

#### **La normativa di riferimento.**

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

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

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

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

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

L'art. 17 bis, commi 8 bis e ter D. Lgs. 141/2010 impone ai suddetti prestatori di servizi di comunicare la loro operatività in Italia, nonché di iscriversi alla **sezione speciale del registro dei cambiavalute tenuto dall'Organismo Agenti e Mediatori** (su cui v. notizia [2022/1\(7\)ES](#)).

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

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

#### **I precedenti giurisprudenziali (e un cenno alla dottrina).**

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

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

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

Anche la giurisprudenza di merito si è espressa in tal senso.

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

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

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

#### **Conclusioni. Il ragionamento della Corte.**

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

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

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

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

Infine, va detto che la pronuncia in commento non si concilia con le previsioni della proposta di **Regolamento sui mercati delle criptovalute** (c.d. MiCAR, acronimo che sta per Markets in Crypto-Assets Regulation: su cui v. notizia [2022/2\(3\)AE](#)), che, da un lato, esclude un obbligo di prospetto per l'offerta di criptovalute e, dall'altro, non assoggetta quest'ultima alle norme sull'offerta a distanza di prodotti finanziari.

EMANUELE STABILE

<https://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snp&id=./20221122/snp@2022@n44378@tS.clean.pdf>

2022/4(14)EB

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

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

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

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

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

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

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

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

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

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

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

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

EMANUELA BURGIO

[https://web.uniroma1.it/deap/sites/default/files/allegati/cass34658\\_22.pdf](https://web.uniroma1.it/deap/sites/default/files/allegati/cass34658_22.pdf)

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

A proposito dell'uso di sistemi algoritmici nell'attività amministrativa (su cui v. in questa Rubrica le notizie [2021/4\(7\)FDA](#) e [2022/1\(13\)FDA](#) a proposito delle *Model Rules* elaborate dallo *European Law Institute* sulla valutazione di impatto delle decisioni algoritmiche nella pubblica amministrazione) si segnala una interessante sentenza del 14 novembre 2022 del TAR Campania – sede di Napoli, Sez. III, n. 7003 sull'uso di sistemi algoritmici nei procedimenti amministrativi per erogare i fondi agricoli gestiti dall'Agenzia per le Erogazioni in Agricoltura (AGEA) per conto della Commissione europea.

Questi i passaggi più significativi della pronuncia.

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

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

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

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

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

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

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

FILIPPO D'ANGELO

2022/4(16)FG

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

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

Si tratta del primo provvedimento cautelare noto di una corte europea che stabilisce che i NFT che riproducono senza autorizzazione i marchi di terzi costituiscono una violazione, concedendo la relativa ingiunzione al titolare dei diritti. Ad oggi, a livello internazionale, sono conosciute solo decisioni similari emesse a Singapore e in Turchia.

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

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

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

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

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

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

Il Tribunale ha rilevato come l'autorizzazione concessa dal giocatore all'utilizzo della propria immagine non escludesse la necessità di chiedere l'autorizzazione anche all'uso dei marchi registrati della squadra di cui erano riprodotte le maglie e la denominazione, in quanto si trattava di beni destinati alla vendita commerciale, in relazione alle quali anche la fama delle diverse squadre in cui il calciatore ha giocato contribuiscono a dare valore all'immagine

digitale da acquistare; come disposto dall'art. 97 della Legge sul Diritto d'Autore, l'uso consentito del diritto all'immagine di una persona non si estende anche all'uso dei marchi rappresentati nella medesima immagine.

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

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

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

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

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

FRANCESCO GROSSI

[https://web.uniroma1.it/deap/sites/default/files/allegati/Trib\\_Roma\\_2022\\_Juve\\_NFT.pdf](https://web.uniroma1.it/deap/sites/default/files/allegati/Trib_Roma_2022_Juve_NFT.pdf)

2022/4(17)EMI

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

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

Nel caso di specie, la Securities Exchange Commission (“**SEC**”) richiedeva un provvedimento cautelare (*summary judgement*) in merito alle attività svolte dalla società del New Hampshire, la LBRY, Inc. (“**LBRY**”), che emette e vende specifici *blockchain token*, dal nome “*LBRY Credits*” o “*LBC*” la cui natura giuridica, e specificamente la loro qualificazione come

*unregistered securities* ai sensi della normativa statunitense applicabile (Sezione 5 del *Securities Act* del 1933), era affermata dalla SEC e negata da LBRY.

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

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

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

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

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

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

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

Sul punto, la Corte, però, ha espressamente sottolineato come risulti necessario analizzare la natura concreta del contratto in esame e che la commistione tra funzione consumeristica di utilità e funzione finanziaria di investimento non escluda la possibilità di qualificare queste operazioni come contratti di investimento, alla luce dei precedenti applicabili al caso di specie e sulla base del c.d. *Howey Test*.

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

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

ENZO MARIA INCUTTI

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

2022/4(18)RMo

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

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

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

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

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

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

caso i dati di localizzazione non sarebbero più stati conservati sui server della società. Google ha omesso di informare gli utenti che, viceversa, anche una volta esclusa tale impostazione, i dati in questione potevano essere raccolti e conservati in altri modi, tra essi, attraverso *Web&App Activity* (che, ad esempio, registra e conserva il dato relativo al luogo in cui un utente compie una ricerca usando Google Search, alla località digitata su Google Maps per ottenere indicazioni stradali, etc.). *Web&App Activity* era preimpostata da Google come attiva, a meno che l'utente non si fosse adoperato per "disabilitarla". Fino al 2018, secondo le allegazioni dell'*Attorney General*, Google non ha reso nota agli utenti l'esistenza di tale ultima impostazione al momento della creazione dell'account e, soprattutto, non ha informato che anche tramite essa la società procedeva alla raccolta e immagazzinamento dei dati di localizzazione. Gli utenti venivano informati dell'esistenza di *Web&App Activity* soltanto al momento di accedere ad una separata pagina online, dove pure, tuttavia, *Location History* veniva indicata come unico mezzo capace di raccogliere e conservare tali dati. Dopo tale data, Google ha bensì cominciato a fare menzione di *Web&App Activity* al momento della creazione dell'account, senza però svelarne la reale funzionalità (informazione, questa, acquisibile soltanto accedendo ad una apposita pagina web per mezzo di un link). Google ha dunque fuorviato i propri utenti non fornendo la ricordata informazione e dando ad intendere che questa forma di trattamento venisse svolta soltanto per mezzo di *Location History*. Inoltre, sempre Google ha falsamente suscitato negli utenti l'affidamento circa la capacità di controllare il trattamento dei dati di localizzazione attraverso l'impostazione del proprio account (con dichiarazioni del seguente tenore "Tu puoi sempre controllare come noi raccogliamo e usiamo questi dati ... Puoi sempre rettificare le tue impostazioni in un secondo momento o revocare il tuo consenso ...").

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

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

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

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

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

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

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

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

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

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

Sono poi introdotte prescrizioni anche con riguardo al c.d. *Account Creation Flaw*, vale a dire alla *user interface* o al processo grazie ai quali viene creato un account: all'atto della creazione di quest'ultimo, Google, non solo deve informare se raccoglie e conserva i suddetti dati, ma deve anche adottare certe modalità di interazione con gli utenti, atte a consigliare a questi ultimi di disattivare le impostazioni che siano attive *by default*.

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

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

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

ROBERTA MONTINARO

2022/4(19)AM-GD**Le due sentenze "gemelle diverse" del Tar Lazio, sede di Roma, Sez. I del 18.11.2022 nei casi riguardanti Apple (sentenza n.15317) e Google (sentenza n.15326) in materia di pratiche commerciali sleali e patrimonializzazione dei dati personali**

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

\*\*\*

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

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

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

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

Con i cinque motivi oggetto di accoglimento Apple aveva contestato: (1) il travisamento fattuale in cui era incorsa l’Autorità ritenendo che la configurazione dell’ID Apple implicasse la raccolta e il trattamento di dati personali degli utenti per finalità commerciali; (2) che la personalizzazione degli Store non dà luogo a cessione dei dati a terzi, né a sfruttamento economico dei dati, basandosi su un numero molto limitato di dati, ed essendo tali solo quelli strettamente necessari per fornire servizi personalizzati; (3) che il comportamento del consumatore medio negli Store non subisce alterazioni in virtù della personalizzazione, giacché, a differenza del caso in cui i servizi siano pubblicizzati come “gratuiti” (ad esempio, servizi di social media o di messaggistica istantanea), gli Store sono negozi digitali per la vendita di contenuti e, finché il consumatore non sceglie consapevolmente di effettuare un acquisto Apple non realizza alcun fatturato; (4) che l’informativa che precede l’accesso agli Store è completa, poiché strutturata in modo tale da rendere gli utenti edotti che i loro dati di acquisto e ricerca possono essere utilizzati per la personalizzazione degli stessi Store; da ciò discende la liceità della Condotta A; (5) che il sistema opt-out di per sé non implica un

indebito condizionamento dell'utente tale da porlo in una condizione coartata che ne pregiudica gli interessi; da ciò discende la liceità della Condotta B.

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

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

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

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

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

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

ANDREA MAREGA

\*\*\*

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

La prima pratica (Condotta A), ritenuta scorretta, riguardava l'omessa informativa circa la raccolta e l'utilizzo dei dati personali degli utenti per finalità commerciali, sia nella fase di creazione dell'account Google (indispensabile per l'utilizzo di tutti i servizi offerti), sia durante l'utilizzo dei servizi offerti da Google (ossia, Google Drive, Google Store, Google Play Store, Google Payments, Google Play Edicola, Google Play Musica, Google Maps, Google Search, Google Traduttore e YouTube).

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

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

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

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

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

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

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

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

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

Per quanto riguarda il terzo motivo, il TAR ha confermato la sanzione di 10 milioni di euro, tenuto conto della notevole dimensione economica del professionista quale leader mondiale nel settore, dell'ampia diffusione delle pratiche tramite internet, nonché del rifiuto

dell'AGCM degli impegni presentati da Google e della necessità di mantenere le due pratiche (Condotta A e Condotta B) separate da un punto di vista strutturale e funzionale.

GIORGIA DIOTALLEVI

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



## INDICI

## INDICI PER ANNI

### ANNO 2020

<a href="#">2020/1(1)RM</a>	
L'utilizzo dei droni ai tempi del coronavirus – La Nota ENAC del 23 marzo 2020 e il successivo stop del Dipartimento della Pubblica Sicurezza del Ministero dell'Interno .....	p. 5
<a href="#">2020/1(2)MP</a>	
Diritto societario e Coronavirus: intervento e verbalizzazione assembleare a distanza .....	p. 6
<a href="#">2020/1(3)EMI</a>	
Regno Unito: quale futuro per crypto-asset e smart contract? .....	p. 7
<a href="#">2020/1(4)MG</a>	
Dati personali e valore economico – il Tar Lazio conferma l'importante provvedimento dell'Antitrust nel caso Facebook .....	p. 8
<a href="#">2020/1(5)SO</a>	
Il Libro Bianco della Commissione Europea del 19 febbraio 2020 sull'Intelligenza Artificiale: “Eccellenza e Fiducia” .....	p. 9
<a href="#">2020/1(6)DI</a>	
Intelligenza Artificiale e Costituzione francese .....	p. 10
<a href="#">2020/1(7)LC</a>	
Rome Call for AI Ethics: Per un'intelligenza artificiale umanistica .....	p. 11
<a href="#">2020/1(8)EWDM</a>	
Le Linee Guide AGID del 23 marzo 2020 - Il valore giuridico della firma con il Sistema Pubblico d'identità Digitale (SPiD) .....	p. 12
<a href="#">2020/2(1)FR</a>	
La Comunicazione della Commissione europea COM(2020) 66 final “Una strategia europea per i dati” .....	p. 13
<a href="#">2020/2(2)CR</a>	
I lavori del 12 maggio 2020 della Commissione giuridica (JURI) del Parlamento Europeo sulla regolazione della Intelligenza Artificiale: il Draft Report sugli aspetti etici .....	p. 15
<a href="#">2020/2(3)SO</a>	
(segue): il Draft Report sulla responsabilità civile .....	p. 16
<a href="#">2020/2(4)LC</a>	
(segue): il Draft Report sulla proprietà intellettuale .....	p. 18
<a href="#">2020/2(5)EMI</a>	
Le linee guida del EDPB sul consenso: chiarimenti su <i>cookie wall</i> e scorrimento dei siti web .....	p. 20
<a href="#">2020/2(6)DI</a>	
Una nuova legge francese sui contenuti offensivi sul web .....	p. 21
<a href="#">2020/2(7)MP</a>	
Il (primo) parere del Garante per la protezione dei dati personali sull'applicazione volta al tracciamento dei contagi da Covid-19 .....	p. 22

<a href="#">2020/2(8)EP</a>	Stablecoin globali: prospettive regolamentari e rischi finanziari sotto la lente della BCE .....	p. 23
<a href="#">2020/3(1)CR</a>	La sentenza “Schrems II” del 16 luglio 2020 della Corte di Giustizia UE sul Privacy Shield con gli USA e sulle clausole contrattuali tipo .....	p. 25
<a href="#">2020/3(2)FB</a>	Le conclusioni dell'Avvocato generale della Corte di Giustizia UE del 16 luglio 2020 sull'interpretazione delle direttive 2001/29/CE e 2000/31/CE sulla responsabilità dei gestori di piattaforme online con riferimento alle opere protette dal diritto d'autore .....	p. 26
<a href="#">2020/3(3)LC</a>	CasaPound vs. Facebook: il Tribunale di Roma conferma in sede di reclamo il provvedimento cautelare a favore di CasaPound .....	p. 30
<a href="#">2020/3(4)FP</a>	Pubblicate il 10 luglio 2020 la relazione introduttiva e le prime tre bozze di relazione del gruppo di esperti dell' <i>Observatory on the Online Platform Economy</i> .....	p. 31
<a href="#">2020/3(5)EWDM</a>	Lo studio del luglio 2020 su “Intelligenza Artificiale e responsabilità civile” commissionato dalla Commissione JURI del Parlamento europeo .....	p. 34
<a href="#">2020/3(6)SG</a>	Il Consiglio di Stato francese conferma la sanzione di 50 milioni di Euro a Google per violazione del GDPR .....	p. 36
<a href="#">2020/3(7)EMI</a>	La « <i>Algorithm Charter</i> » della Nuova Zelanda .....	p. 37
<a href="#">2020/4(1)SG</a>	La risoluzione del Parlamento europeo del 20 ottobre 2020 sul regime di responsabilità civile per l'intelligenza artificiale .....	p. 39
<a href="#">2020/4(2)MS</a>	La proposta della Commissione europea del 24 settembre 2020 avente ad oggetto l'emanazione di un Regolamento Europeo sui Mercati di Cripto-attività (MiCAR) .....	p. 41
<a href="#">2020/4(3)MP</a>	La prima sentenza della Corte di Giustizia UE sul principio di «neutralità di Internet» ai sensi del regolamento (UE) 2015/2120 .....	p. 44
<a href="#">2020/4(4)CM</a>	La lunga marcia verso il GDPR cinese: la prima legge sulla protezione delle informazioni personali della Repubblica popolare nella bozza per i commenti pubblici del 21 ottobre 2020 .....	p. 46
<a href="#">2020/4(5)CR</a>	Le FAQ del Garante Privacy italiano dell'ottobre 2020 per la protezione dei dati personali sulla refertazione online .....	p. 47
<a href="#">2020/4(6)DPDM</a>	La nuova indagine della Commissione europea per abuso di posizione dominante di Amazon .....	p. 48
<a href="#">2020/4(7)LC</a>	Droits voisins e snippets: la Corte d'appello di Parigi conferma la decisione dell'Autorità garante della concorrenza francese nei confronti di Google .....	p. 49

[2020/4\(8\)SO](#)

La Sapienza sottoscrive “Rome Call for AI Ethics” ..... p. 50

**ANNO 2021**

[2021/1\(1\)DPDM](#)

La “rivoluzione digitale” e lo European Democracy Action Plan del 03.12.2020 ..... p. 57

[2021/1\(2\)GC](#)

La strategia digitale della Risoluzione del Parlamento Europeo del 25.11.2020 “Verso un mercato unico più sostenibile per le imprese e i consumatori” ..... p. 58

[2021/1\(3\)ST](#)

Verso il Digital Services Act: la Proposta di Regolamento sul “mercato unico dei servizi digitali” del 15.12.2020 ..... p. 59

[2021/1\(4\)EMI](#)

Verso il Digital Markets Act: la Proposta di Regolamento su “mercati equi e contendibili nel settore digitale” del 15.12.2020 ..... p. 65

[2021/1\(5\)RMo](#)

Il parere del 10.02.2021 dello EDPS sulla proposta del Digital Services Act in particolare sulla pubblicità mirata e i recommender systems ..... p. 65

[2021/1\(6\)LC](#)

La Risoluzione del 21.01.2021 del Parlamento europeo sul diritto dei lavoratori alla disconnessione ..... p. 67

[2021/1\(7\)ER](#)

Regolamento P2B e nuove funzioni delle Autorità indipendenti alla luce della Legge di Bilancio 2021 ..... p. 68

[2021/1\(8\)CR](#)

Clearview AI condannata in Germania per violazione del GDPR: il caso Marx ..... p. 69

[2021/1\(9\)CM](#)

Apple condannata dal Tribunale di Milano a fornire accesso al patrimonio digitale di un defunto (ordinanza del 09.02.2021) ..... p. 70

[2021/2\(1\)SO](#)

Verso l’Artificial Intelligence Act: la Proposta di Regolamento del 21.04.2021 su regole armonizzate in materia di intelligenza artificiale ..... p. 72

[2021/2\(2\)CR](#)

Il comunicato del 23.04.2021 dello EDPS sulla proposta dell’*Artificial Intelligence Act* in particolare sul riconoscimento facciale ..... p. 79

[2021/2\(3\)CR](#)

Il parere del Garante Privacy del 16.04.2021 sul sistema di riconoscimento facciale SARI Real Time da parte del Ministero dell’Interno ..... p. 80

[2021/2\(4\)FP](#)

Lo studio del 05.02.2021 pubblicato dal Parlamento europeo sulla responsabilità delle piattaforme online ..... p. 81

[2021/2\(5\)FP](#)

I Final Reports del marzo 2021 del gruppo di esperti dell’Osservatorio sulla platform economy ..... p. 83

<a href="#">2021/2(6)EP</a>	Il Parere della BCE del 19.02.2021 sulla Proposta di Regolamento sui mercati di crypto-assets .....	p. 85
<a href="#">2021/2(7)EP</a>	Il comunicato di Consob e Banca d'Italia sui crypto-assets del 28.04.2021 .....	p. 87
<a href="#">2021/2(8)MG</a>	La sentenza 2631 del Consiglio di Stato del 29.03.2021 nel caso Facebook (gratuità del servizio e divieto di pratiche commerciali scorrette) .....	p. 88
<a href="#">2021/2(9)DPDM</a>	La comunicazione di addebiti del 30.04.2021 della Commissione europea ad Apple per abuso di posizione dominante per le regole delle app di musica in streaming su App Store .....	p. 89
<a href="#">2021/2(10)EMI</a>	Fair use e open source: la decisione della Corte Suprema degli Stati Uniti d'America del 05.04.2021 nel caso delle API di Java (Oracle c/ Google) .....	p. 90
<a href="#">2021/3(1)DI</a>	La Carta dei diritti digitali presentata dal Governo spagnolo il 14 luglio 2021..	p. 92
<a href="#">2021/3(2)SO-CS</a>	La Corte di Cassazione subordina la validità del consenso al trattamento dei dati personali alla trasparenza dell'algoritmo che governa il servizio per il quale il consenso è prestato (ordinanza 14381 del 25 maggio 2021 a proposito di un servizio di calcolo del c.d. <i>rating</i> reputazionale) .....	p. 93
<a href="#">2021/3(3)CR</a>	Il pronunciamento congiunto EDPS - EDPB del 21 giugno 2021 sulla proposta di disciplina sul riconoscimento facciale contenuta nell' <i>Artificial Intelligence Act</i> .....	p. 95
<a href="#">2021/3(4)CM</a>	Le regole sul riconoscimento facciale per le società private emesse dalla Suprema Corte del Popolo della Repubblica Popolare Cinese il 28 luglio 2021	p. 97
<a href="#">2021/3(5)LV</a>	Le Linee Guida EDPB del 7 luglio 2021 sugli assistenti vocali virtuali .....	p. 98
<a href="#">2021/3(6)CR</a>	Le Linee Guida del Garante Privacy italiano sui cookies ed altri strumenti di tracciamento del 10 giugno 2021 .....	p. 100
<a href="#">2021/3(7)AF</a>	La decisione del Consiglio direttivo della BCE del 12 luglio 2021 di avviare l'analisi del progetto per un "euro digitale" .....	p. 102
<a href="#">2021/3(8)FP</a>	La Repubblica di El Salvador adotta il Bitcoin come moneta avente corso legale nel Paese (la " <i>Ley Bitcoin</i> " dell'8 giugno 2021) .....	p. 103
<a href="#">2021/3(9)AN</a>	Il provvedimento del 22 luglio 2021 del Garante Privacy nei confronti di Deliveroo per il trattamento dei dati personali dei riders .....	p. 106
<a href="#">2021/3(10)CM</a>	Il pronunciamento del 28 maggio 2021 della Suprema Corte del Popolo della Repubblica Popolare Cinese sul valore probatorio dei dati registrati su blockchain .....	p. 108

<a href="#">2021/4(1)FB</a>	
Il recepimento in Italia delle direttive (UE) 2019/770 e 2019/771 relative a determinati aspetti dei contratti di fornitura di contenuti e servizi digitali e a determinati aspetti dei contratti di vendita di beni di consumo .....	p. 108
<a href="#">2021/4(2)FP</a>	
Il recepimento in Germania della direttiva (UE) 2019/770 .....	p. 114
<a href="#">2021/4(3)CR</a>	
Le rilevanti modifiche al Codice Privacy introdotte dal ‘Decreto Capienze’ del 7 ottobre 2021 come convertito in legge con modifiche ad opera della legge 3 dicembre 2021 n. 205 .....	p. 117
<a href="#">2021/4(4)RA</a>	
Verso il Data Governance Act: le modifiche del Consiglio dell’Unione Europea del 24 settembre 2021 alla proposta di regolamento della Commissione, approvate dal Comitato dei rappresentanti permanenti il 1 ottobre 2021 con contestuale mandato alla Presidenza del Consiglio di avviare le negoziazioni con il Parlamento Europeo .....	p. 119
<a href="#">2021/4(5)EMI</a>	
La sentenza della Corte di Giustizia UE del 6 ottobre 2021 sul diritto di decompilazione del software (il caso <i>Top System</i> ) .....	p. 123
<a href="#">2021/4(6)FG</a>	
La sentenza della Court of Appeal del 21 settembre sul caso Dabus: l’intelligenza artificiale può essere considerata inventore? .....	p. 125
<a href="#">2021/4(7)FDA</a>	
La sentenza del Tar Lazio n. 7589 del 24 giugno 2021 su algoritmi e attività amministrativa (a proposito di procedure di mobilità nella Pubblica Amministrazione) .....	p. 128
<a href="#">2021/4(8)VR</a>	
L’ordinanza del 16 settembre 2021 del Garante Privacy a proposito del sistema software di supervisione degli studenti “Respondus” impiegato dall’Università Bocconi di Milano per le prove scritte di esame .....	p. 129
<a href="#">2021/4(9)ES</a>	
L’apertura della prima finestra temporale sulla sandbox regolamentare per i progetti fintech di cui al Decreto del MEF n. 100 del 30 aprile 2021 .....	p. 133
<a href="#">2021/4(10)AF</a>	
Il rapporto del 13 ottobre 2021 dei Ministeri dell’Economia e delle Banche Centrali dei Paesi G7 “ <i>Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)</i> ” .....	p. 135
<a href="#">2021/4(11)SS</a>	
Le Classi di rischio dei ‘Software As Medical Devices’ (SAMDs) alla data di piena applicazione del Regolamento 2017/745 UE sui dispositivi medicali .....	p. 137
<a href="#">2021/4(12)BC</a>	
La legge dello Stato del <i>Wyoming</i> sulle <i>Decentralized Assets Organizations</i> (DAOs) del 21 aprile 2021 .....	p. 138
<a href="#">2021/4(13)CM</a>	
La prima legge sulla protezione delle informazioni personali della Repubblica Popolare Cinese (la ‘PIPL’) .....	p. 141

## ANNO 2022

### [2022/1\(1\)EB](#)

L'attuazione della direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (D.Lgs. 8 novembre 2021, n. 177) ..... p. 149

### [2022/1\(2\)RA](#)

L'attuazione della direttiva “Open Data” (UE) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (D.Lgs. 8 novembre 2021, n. 200, modificativo del D.Lgs. 36/2006) ..... p. 152

### [2022/1\(3\)EMI](#)

L'attuazione della direttiva (UE) 2018/1972 che istituisce il Codice europeo delle comunicazioni elettroniche (D.Lgs. 8 novembre 2021, n. 207, modificativo del D. Lgs. 259/2003) ..... p. 155

### [2022/1\(4\)SO](#)

Verso il Data Act: la proposta di Regolamento del Parlamento e del Consiglio su regole armonizzate sull'accesso equo e l'uso dei dati (legge sui dati) COM(2022) 68 final del 23 febbraio 2022 ..... p. 156

### [2022/1\(5\)ST](#)

La proposta di Dichiarazione europea sui diritti e i principi digitali per il decennio digitale COM(2022) 28 final del 26 gennaio 2022 ..... p. 160

### [2022/1\(6\)SO](#)

La proposta di Regolamento del Parlamento e del Consiglio relativo alla trasparenza e al targeting della pubblicità politica COM(2021) 731 final del 25 novembre 2021 ..... p. 163

### [2022/1\(7\)ES](#)

Il Decreto del Ministero dell'economia e delle finanze del 13 gennaio 2022 sull'iscrizione alla sezione speciale del registro dei cambiavalute da parte dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale ..... p. 165

### [2022/1\(8\)GDI](#)

La decisione del 10 febbraio 2022 del Garante privacy italiano sul trattamento di dati biometrici da parte di Clearview AI ..... p. 167

### [2022/1\(9\)CR](#)

La decisione del 13 gennaio 2022 del Garante privacy austriaco sul trasferimento di dati personali negli USA per Google Analytics ..... p. 168

### [2022/1\(10\)CR](#)

La decisione del 10 febbraio 2022 del Garante privacy francese sul trasferimento di dati personali negli USA per Google Analytics ..... p. 170

### [2022/1\(11\)VR](#)

La decisione del 2 febbraio 2022 del garante privacy belga sul Real Time Bidding e le attività di online advertising a proposito del Quadro di Trasparenza e Consenso elaborato e gestito da IAB Europe ..... p. 171

### [2022/1\(12\)FG](#)

La sentenza della Cassazione n. 3952 del 8 febbraio 2022 sul diritto all'oblio e le copie cache ..... p. 177

### [2022/1\(13\)FDA](#)

Le “Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration” dello *European Law Institute* (ELI) del 3 marzo 2022 ..... p. 179

<a href="#">2022/2(1)RA</a>	Approvato il ‘Data Governance Act’: Regolamento (UE) 2022/868 del 30 maggio 2022 sulla governance europea dei dati .....	p. 181
<a href="#">2022/2(2)BC</a>	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 .....	p. 187
<a href="#">2022/2(3)AF</a>	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 ..	p. 191
<a href="#">2022/2(4)FG</a>	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 <i>copyright</i> nel mercato unico digitale (Causa C-401/19) .....	p. 192
<a href="#">2022/2(5)SO</a>	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: il documento pubblicato il 28 giugno 2022 dallo <i>UK Intellectual Property Office</i> .....	p. 196
<a href="#">2022/2(6)EMI</a>	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) .....	p. 198
<a href="#">2022/2(7)VR</a>	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. <i>law enforcement directive</i> .....	p. 200
<a href="#">2022/2(8)ES</a>	Il Parere della BCE del 29 dicembre 2021 sulla proposta di regolamento sull’intelligenza artificiale ( <i>‘Artificial Intelligence Act’</i> ) .....	p. 205
<a href="#">2022/2(9)ES</a>	Il Regolamento di Banca d’Italia del 22 marzo 2022 sul trattamento dei dati personali effettuato nell’ambito della sua gestione degli esposti .....	p. 208
<a href="#">2022/2(10)AAM</a>	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” .....	p. 211
<a href="#">2022/2(11)AF</a>	La proposta di uno <i>‘US Stablecoin Trust Act’</i> del U.S. <i>Senate Banking Committee</i> del 6 aprile 2022 .....	p. 213
<a href="#">2022/2(12)VP</a>	Il Libro Bianco 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) .....	p. 214

<a href="#">2022/3(1)TDMCDV</a>	
Verso la AI Liability Directive: la proposta della Commissione europea del 28 settembre 2022 per una direttiva sull'adattamento delle regole di responsabilità civile all'Intelligenza Artificiale .....	p. 217
<a href="#">2022/3(2)TDMCDV</a>	
Verso la nuova Product Liability Directive: la proposta della Commissione europea del 28 settembre 2022 per una nuova direttiva sulla responsabilità da prodotto difettoso che abroga la Direttiva 85/374/CEE .....	p. 220
<a href="#">2022/3(3)RA</a>	
Proposta di Regolamento riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo ( <i>Data Act</i> ): <i>First Presidency compromise text</i> del 12 luglio 2022 .....	p. 222
<a href="#">2022/3(4)VR</a>	
La proposta di Regolamento UE sui requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali (c.d. Cyber Resilience Act) .....	p. 226
<a href="#">2022/3(5)EMI</a>	
Verso il regolamento europeo di progettazione eco-sostenibile dei dispositivi mobili tecnologici .....	p. 230
<a href="#">2022/3(6)ES</a>	
Gli ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection .....	p. 232
<a href="#">2022/3(7)FG</a>	
Il parere congiunto EDPB-EDPS n.4/2022 del 28.7.2022 sulla proposta di regolamento della Commissione Europea del 11.05.2022 che stabilisce norme per prevenire e combattere l'abuso sessuale dei minori .....	p. 237
<a href="#">2022/3(8)CR</a>	
NOYB denuncia Google alla CNIL per l'invio di e-mail pubblicitarie non richieste senza consenso degli utenti .....	p. 239
<a href="#">2022/3(9)CR</a>	
Il Garante privacy esprime parere negativo sullo schema di decreto sull'Ecosistema Dati Sanitari (parere del 22.8.2022) .....	p. 240
<a href="#">2022/3(10)LC</a>	
Accesso ai risultati della ricerca scientifica finanziata con fondi federali: nuove linee guida negli Stati Uniti d'America .....	p. 241
<a href="#">2022/3(11)AF</a>	
Le proposte normative dell'11 ottobre 2022 del <i>Financial Stability Board</i> in materia di cripto-attività e <i>global stablecoins</i> .....	p. 243
<a href="#">2022/4(1)ST</a>	
Approvato il Digital Services Act (DSA): Regolamento (UE) 2022/2065 del 19.10.2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE .....	p. 245
<a href="#">2022/4(2)VR</a>	
Approvato il Digital Markets Act (DMA): Regolamento (UE) 2022/1925 del 14.09.2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive 2019/1937/UE e 2020/1828/UE .....	p. 249
<a href="#">2022/4(3)ES</a>	
Approvato il 'DORA': Regolamento (UE) 2022/2554 del 14.12.2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i	

regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 .....	p. 253
<a href="#">2022/4(4)SO</a>	
Le modifiche apportate alla disciplina dell'abuso di dipendenza economica di cui alla legge sulla subfornitura, con decorrenza dal 31 ottobre 2022 .....	p. 256
<a href="#">2022/4(5)RA</a>	
La EU Interinstitutional declaration on digital rights and principles del 14.11.2022 .....	p. 257
<a href="#">2022/4(6)DI</a>	
Il codice deontologico "rafforzato" del 2022 di buone pratiche contro la disinformazione .....	p. 259
<a href="#">2022/4(7)ST</a>	
NetChoice LLC v. Paxton , n. 21-51178- United States Court of Appeals for the Fifth Circuit, provvedimento del 16.9.2022: libertà di parola <i>versus</i> moderazione di contenuti da parte delle piattaforme <i>online</i> .....	p. 261
<a href="#">2022/4(8)CR</a>	
La sentenza CGUE del 20.10.2022 nella causa C 77/21 sui principi di limitazione delle finalità e di limitazione della conservazione ex art. 5 lett. b) ed e) GDPR .....	p. 263
<a href="#">2022/4(9)CAT</a>	
La sentenza CGUE del 27.10.2022 nella causa C-129/21 Proximus (Annuaire électroniques publics) sulle misure da adottarsi da parte del titolare del trattamento di dati personali per informare i motori di ricerca in Internet di una richiesta di cancellazione rivoltagli dall'interessato .....	p. 265
<a href="#">2022/4(10)FDA</a>	
Verso l'Interoperable Europe Act: la proposta della Commissione di regolamento europeo sull'interoperabilità nel settore pubblico del 18.11.2022	p. 267
<a href="#">2022/4(11)SO</a>	
I comunicati del Garante privacy italiano del 18.10.2022, del 21.10.2022 e del 12.11.2022 di avvio di istruttorie a carico di testate editoriali online per iniziative di <i>cookie wall</i> e monetizzazione di dati personali .....	p. 268
<a href="#">2022/4(12)VR</a>	
Il comunicato del 14.11.2022 del Garante privacy italiano di avvio di istruttorie per i sistemi di videosorveglianza dei Comuni di Lecce e di Arezzo .....	p. 269
<a href="#">2022/4(13)ES</a>	
La sentenza Cassazione Sez. 2 Penale n. 44378/2022 del 26.10.2022 sulla qualificazione della moneta virtuale e delle Initial Coin Offerings (a proposito di un sequestro penale preventivo di wallet contenente bitcoin e di una fattispecie di reato di abusivismo finanziario ai sensi dell'art. 166 co. 1 TUF) ..	p. 270
<a href="#">2022/4(14)EB</a>	
L'Ordinanza della Cassazione Prima Sez. Civile n. 34658/2022 del 24.11.2022 sul diritto all'oblio e l'ordine di rimozione c.d. globale (regime Codice privacy anteriore al GDPR) .....	p. 273
<a href="#">2022/4(15)FDA</a>	
La sentenza Tar Campania, sede di Napoli, Sez. III, n. 7003 del 14 novembre 2022 sull'uso di sistemi algoritmici nei procedimenti amministrativi .....	p. 275
<a href="#">2022/4(16)FG</a>	
L'ordinanza del Tribunale di Roma del 20.7.2022 su NFT: il caso della Juventus .....	p. 276

[2022/4\(17\)EMI](#)

L'order del 7.11.2022 della District Court of New Hampshire (USA) sulla qualificazione di un utility token come security ..... p. 277

[2022/4\(18\)RMo](#)

L'Assurance of voluntary compliance tra Google e lo Stato della Pennsylvania (USA) del 14.12.2022 sui dati di localizzazione ..... p. 279

[2022/4\(19\)AM-GD](#)

Le due sentenze "gemelle diverse" del Tar Lazio, sede di Roma, Sez. I del 18.11.2022 nei casi riguardanti Apple (sentenza n.15317) e Google (sentenza n.15326) in materia di pratiche commerciali sleali e patrimonializzazione dei dati personali ..... p. 282

## INDICE PER AUTORE

### **RICCARDO ALFONSI (RA)**

[2021/4\(4\)RA](#)

Verso il Data Governance Act: le modifiche del Consiglio dell'Unione Europea del 24 settembre 2021 alla proposta di regolamento della Commissione, approvate dal Comitato dei rappresentanti permanenti il 1 ottobre 2021 con contestuale mandato alla Presidenza del Consiglio di avviare le negoziazioni con il Parlamento Europeo

[2022/1\(2\)RA](#)

L'attuazione della direttiva "Open Data" (UE) 2019/1024, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (D.Lgs. 8 novembre 2021, n. 200, modificativo del D.Lgs. 36/2006)

[2022/2\(1\)RA](#)

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

[2022/3\(3\)RA](#)

Proposta di Regolamento riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (Data Act): First Presidency compromise text del 12 luglio 2022

[2022/4\(5\)RA](#)

La EU Interinstitutional declaration on digital rights and principles del 14.11.2022

### **FRANCESCO BERNARDI (FB)**

[2020/3\(2\)FB](#)

Le conclusioni dell'Avvocato generale della Corte di Giustizia UE del 16 luglio 2020 sull'interpretazione delle direttive 2001/29/CE e 2000/31/CE sulla responsabilità dei gestori di piattaforme online con riferimento alle opere protette dal diritto d'autore

### **FRANCESCA BERTELLI (FBe)**

[2021/4\(1\)FBe](#)

Il recepimento in Italia delle direttive (UE) 2019/770 e 2019/771 relative a determinati aspetti dei contratti di fornitura di contenuti e servizi digitali e a determinati aspetti dei contratti di vendita di beni di consumo

### **EMANUELA BURGIO (EB)**

[2022/1\(1\)EB](#)

L'attuazione della direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (D.Lgs. 8 novembre 2021, n. 177)

[2022/4\(14\)EB](#)

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

**GIUSEPPINA CAPALDO (GC)**

[2021/1\(2\)GC](#)

La strategia digitale della Risoluzione del Parlamento Europeo del 25.11.2020  
“*Verso un mercato unico più sostenibile per le imprese e i consumatori?*”

**LUCIO CASALINI (LC)**

[2020/1\(7\)LC](#)

Rome Call for AI Ethics: Per un'intelligenza artificiale umanistica

[2020/2\(4\)LC](#)

(segue): il *Draft report sulla proprietà intellettuale*

[2020/3\(3\)LC](#)

CasaPound vs. Facebook: il Tribunale di Roma conferma in sede di reclamo  
il provvedimento cautelare a favore di CasaPound

[2020/4\(7\)LC](#)

*Droits voisins e snippets*: la Corte d'appello di Parigi conferma la decisione  
dell'Autorità garante della concorrenza francese nei confronti di Google

[2021/1\(6\)LC](#)

La Risoluzione del 21.01.2021 del Parlamento europeo sul diritto dei  
lavoratori alla disconnessione

[2022/3\(10\)LC](#)

Accesso ai risultati della ricerca scientifica finanziata con fondi federali: nuove  
linee guida negli Stati Uniti d'America

**BENEDETTO COLOSIMO (BC)**

[2021/4\(12\)BC](#)

La legge dello Stato del Wyoming sulle Decentralized Assets Organizations  
(DAOs) del 21 aprile 2021

[2022/2\(2\)BC](#)

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

**FILIPPO D'ANGELO (FDA)**

[2021/4\(7\)FDA](#)

La sentenza del Tar Lazio n. 7589 del 24 giugno 2021 su algoritmi e attività  
amministrativa (a proposito di procedure di mobilità nella Pubblica  
Amministrazione)

[2022/1\(13\)FDA](#)

Le “Model Rules on Impact Assessment of Algorithmic Decision-Making  
Systems Used by Public Administration” dello European Law Institute (ELI)  
del 3 marzo 2022

[2022/4\(10\)FDA](#)

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

[2022/4\(15\)FDA](#)

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

**TOMMASO DE MARI CASARETO DAL VERME (TDMCDV)**

[2022/3\(1\)TDMCDV](#)

Verso la AI Liability Directive: la proposta della Commissione europea del 28 settembre 2022 per una direttiva sull'adattamento delle regole di responsabilità civile all'Intelligenza Artificiale

[2022/3\(2\)TDMCDV](#)

Verso la nuova Product Liability Directive: la proposta della Commissione europea del 28 settembre 2022 per una nuova direttiva sulla responsabilità da prodotto difettoso che abroga la Direttiva 85/374/CEE

**DOMENICO PIERS DE MARTINO (DPDM)**

[2020/4\(6\)DPDM](#)

La nuova indagine della Commissione europea per abuso di posizione dominante di Amazon

[2021/1\(1\)DPDM](#)

La "rivoluzione digitale" e lo *European Democracy Action Plan* del 03.12.2020.

[2021/2\(9\)DPDM](#)

La comunicazione di addebiti del 30.04.2021 della Commissione europea ad Apple per abuso di posizione dominante per le regole delle app di musica in *streaming* su App Store

**GIORGIA DIOTALLEVI (GD)**

[2022/4\(19\)AM-GD](#)

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

**GUIDO D'IPPOLITO (GDI)**

[2022/1\(8\)GDI](#)

La decisione del 10 febbraio 2022 del garante privacy italiano sul trattamento di dati biometrici da parte di Clearview AI

**ETTORE WILLIAM DI MAURO (EWDM)**

[2020/1\(8\)EWDM](#)

Le Linee Guide AGID del 23 marzo 2020 - Il valore giuridico della firma con il Sistema Pubblico d'identità Digitale (SPiD)

[2020/3\(5\)EWDM](#)

Lo studio del luglio 2020 su "Intelligenza Artificiale e responsabilità civile" commissionato dalla Commissione JURI del Parlamento europeo

**ALICE FILIPPETTA (AF)**

[2021/3\(7\)AF](#)

La decisione del Consiglio direttivo della BCE del 12 luglio 2021 di avviare l'analisi del progetto per un "euro digitale"

[2021/4\(10\)AF](#)

Il rapporto del 13 ottobre 2021 dei Ministeri dell'Economia e delle Banche Centrali dei Paesi G7 "Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)"

[2022/2\(3\)AF](#)

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

[2022/2\(11\)AF](#)

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

[2022/3\(11\)AF](#)

Le proposte normative dell'11 ottobre 2022 del Financial Stability Board in materia di cripto-attività e global stablecoins

#### **SARA GARREFFA (SG)**

[2020/3\(6\)SG](#)

Il Consiglio di Stato francese conferma la sanzione di 50 milioni di Euro a Google per violazione del GDPR

[2020/4\(1\)SG](#)

La risoluzione del Parlamento europeo del 20 ottobre 2020 sul regime di responsabilità civile per l'intelligenza artificiale

#### **MARISTELLA GIANNINI (MG)**

[2020/1\(4\)MG](#)

Dati personali e valore economico – il Tar Lazio conferma l'importante provvedimento dell'Antitrust nel caso Facebook

[2021/2\(8\)MG](#)

La sentenza 2631 del Consiglio di Stato del 29.03.2021 nel caso Facebook (gratuità del servizio e divieto di pratiche commerciali scorrette)

#### **FRANCESCO GROSSI (FG)**

[2021/4\(6\)FG](#)

La sentenza della *Court of Appeal* del 21 settembre sul caso Dabus: l'intelligenza artificiale può essere considerata inventore?

[2022/1\(12\)FG](#)

La sentenza della Cassazione n. 3952 del 8 febbraio 2022 sul diritto all'oblio e le copie cache

[2022/2\(4\)FG](#)

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)

[2022/3\(7\)FG](#)

Il parere congiunto EDPB-EDPS sulla proposta di regolamento della Commissione Europea del 11.05.2022 che stabilisce norme per prevenire e combattere l'abuso sessuale dei minori

[2022/4\(16\)FG](#)

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

#### **DANIELE IMBRUGLIA (DI)**

[2020/1\(6\)DI](#)

Intelligenza Artificiale e Costituzione francese

[2020/2\(6\)DI](#)

Una nuova legge francese sui contenuti offensivi sul web

[2021/3\(1\)DI](#)

La Carta dei diritti digitali presentata dal Governo spagnolo il 14 luglio 2021

### **ENZO MARIA INCUTTI (EMI)**

[2020/1\(3\)EMI](#)

Regno Unito: quale futuro per *crypto-asset* e *smart contract*?

[2020/2\(5\)EMI](#)

Le linee guida del EDPB sul consenso: chiarimenti su *cookie wall* e scorrimento dei siti web

[2020/3\(7\)EMI](#)

La «*Algorithm Charter*» della Nuova Zelanda

[2021/1\(4\)EMI](#)

Verso il *Digital Markets Act*: la Proposta di Regolamento su “mercati equi e contendibili nel settore digitale” del 15.12.2020

[2021/2\(10\)EMI](#)

*Fair use* e *open source*: la decisione della Corte Suprema degli Stati Uniti d’America del 05.04.2021 nel caso della API di Java (Oracle c/ Google)

[2021/4\(5\)EMI](#)

La sentenza della Corte di Giustizia UE del 6 ottobre 2021 sul diritto di decompilazione del software (il caso Top System)

[2022/1\(3\)EMI](#)

L’attuazione della direttiva (UE) 2018/1972 che istituisce il Codice europeo delle comunicazioni elettroniche (D. Lgs. 8 novembre 2021, n. 207, modificativo del D. Lgs. 259/2003)

[2022/2\(6\)EMI](#)

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)

[2022/3\(5\)EMI](#)

Verso il regolamento europeo di progettazione eco-sostenibile dei dispositivi mobili tecnologici

[2022/4\(17\)EMI](#)

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

### **ROSARIA MANAGÒ (RM)**

[2020/1\(1\)RM](#)

L’utilizzo dei droni ai tempi del coronavirus – La Nota ENAC del 23 marzo 2020 e il successivo stop del Dipartimento della Pubblica Sicurezza del Ministero dell’Interno

**ANDREA MAREGA (AM)**

[2022/4\(19\)AM-GD](#)

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

**ANNA ANITA MOLLO (AAM)**

[2022/2\(10\)AAM](#)

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”

**ROBERTA MONTINARO (RMO)**

[2021/1\(5\)RMO](#)

Il parere del 10.02.2021 dello *European Data Protection Advisor* sulla proposta del *Digital Services Act* in particolare sulla pubblicità mirata e i *recommender systems*

[2022/4\(18\)RMO](#)

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

**CORRADO MORICONI (CM)**

[2020/4\(4\)CM](#)

La lunga marcia verso il *GDPR* cinese: la prima legge sulla protezione delle informazioni personali della Repubblica popolare nella bozza per i commenti pubblici del 21 ottobre 2020

[2021/1\(9\)CM](#)

Apple condannata dal Tribunale di Milano a fornire accesso al patrimonio digitale di un defunto (ordinanza del 09.02.2021)

[2021/3\(4\)CM](#)

Le regole sul riconoscimento facciale per le società private emesse dalla Suprema Corte del Popolo della Repubblica Popolare Cinese il 28 luglio 2021.

[2021/3\(10\)CM](#)

Il pronunciamento del 28 maggio 2021 della Suprema Corte del Popolo della Repubblica Popolare Cinese sul valore probatorio dei dati registrati su blockchain

[2021/4\(13\)CM](#)

La prima legge sulla protezione delle informazioni personali della Repubblica Popolare Cinese (la ‘PIPL’)

**ARIANNA NERI (AN)**

[2021/3\(9\)AN](#)

Il provvedimento del 22 luglio 2021 del Garante Privacy nei confronti di Deliveroo per il trattamento dei dati personali dei riders

## **SALVATORE ORLANDO (SO)**

[2020/1\(5\)SO](#)

Il Libro Bianco della Commissione Europea del 19 febbraio 2020 sull'Intelligenza Artificiale: "Eccellenza e Fiducia"

[2020/2\(3\)SO](#)

(segue): il *Draft report sulla responsabilità civile*

[2020/4\(8\)SO](#)

La Sapienza aderisce alla "Rome Call for AI Ethics"

[2021/2\(1\)SO](#)

Verso l'*Artificial Intelligence Act*: la Proposta di Regolamento del 21.04.2021 su regole armonizzate in materia di intelligenza artificiale

[2021/3\(2\)SO-CS](#)

La Corte di Cassazione subordina la validità del consenso al trattamento dei dati personali alla trasparenza dell'algoritmo che governa il servizio per il quale il consenso è prestato (ordinanza 14381 del 25 maggio 2021 a proposito di un servizio di calcolo del c.d rating reputazionale)

[2022/1\(4\)SO](#)

Verso il Data Act: la proposta di Regolamento del Parlamento e del Consiglio su regole armonizzate sull'accesso equo e l'uso dei dati (legge sui dati) COM(2022) 68 final del 23.2.2022

[2022/1\(6\)SO](#)

La proposta di Regolamento del Parlamento e del Consiglio relativo alla trasparenza e al targeting della pubblicità politica COM(2021) 731 final del 25 novembre 2021

[2022/2\(5\)SO](#)

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

[2022/4\(4\)SO](#)

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

[2022/4\(11\)SO](#)

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

## **MICHELA PAGANELLI (MP)**

[2020/1\(2\)MP](#)

Diritto societario e Coronavirus: intervento e verbalizzazione assembleare a distanza

[2020/2\(7\)MP](#)

Il (primo) parere del Garante per la protezione dei dati personali sull'applicazione volta al tracciamento dei contagi da Covid-19

[2020/4\(3\)MP](#)

La prima sentenza della Corte di Giustizia UE sul principio di «neutralità di Internet» ai sensi del regolamento (UE) 2015/2120

### **FEDERICO PISTELLI (FP)**

[2020/3\(4\)FP](#)

Pubbligate il 10 luglio 2020 la relazione introduttiva e le prime tre bozze di relazione del gruppo di esperti dell'*Observatory on the Online Platform Economy*

[2021/2\(4\)FP](#)

Lo studio del 05.02.2021 pubblicato dal Parlamento europeo sulla responsabilità delle piattaforme *online*

[2021/2\(5\)FP](#)

I *Final Reports* del marzo 2021 del gruppo di esperti dell'Osservatorio sulla *platform economy*

[2021/3\(8\)FP](#)

La Repubblica di El Salvador adotta il Bitcoin come moneta avente corso legale nel Paese (la "Ley Bitcoin" dell'8 giugno 2021)

[2021/4\(2\)FP](#)

Il recepimento in Germania della direttiva (UE) 2019/770

### **VICENZO PITTELLI (VP)**

[2022/2\(12\)VP](#)

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)

### **EUGENIO PROSPERI (EP)**

[2020/2\(8\)EP](#)

*Stablecoin* globali: prospettive regolamentari e rischi finanziari sotto la lente della BCE

[2021/2\(6\)EP](#)

Il Parere della BCE del 19.02.2021 sulla Proposta di Regolamento sui mercati di crypto-assets

[2021/2\(7\)EP](#)

Il comunicato di Consob e Banca d'Italia sui crypto-assets del 28.04.2021

### **CHIARA RAUCCIO (CR)**

[2020/2\(2\)CR](#)

I lavori del 12 maggio 2020 della Commissione giuridica (JURI) del Parlamento Europeo sulla regolazione della Intelligenza Artificiale: il *Draft Report* sugli aspetti etici

[2020/3\(1\)CR](#)

La sentenza "Schrems II" del 16 luglio 2020 della Corte di Giustizia UE sul Privacy Shield con gli USA e sulle clausole contrattuali tipo

[2020/4\(5\)CR](#)

Le FAQ del Garante per la protezione dei dati personali sulla refertazione online

[2021/1\(8\)CR](#)

Clearview AI condannata in Germania per violazione del GDPR: il caso Marx

[2021/2\(2\)CR](#)

*Il comunicato del 23.04.2021 dello European Data Protection Supervisor sulla proposta dell'Artificial Intelligence Act in particolare sul riconoscimento facciale*

[2021/2\(3\)CR](#)

Il parere del Garante Privacy del 25.03.2021 sul sistema di riconoscimento facciale SARI Real Time da parte del Ministero dell'Interno

[2021/3\(3\)CR](#)

Il pronunciamento congiunto EDPS - EDPB del 21 giugno 2021 sulla proposta di disciplina sul riconoscimento facciale contenuta nell'Artificial Intelligence Act

[2021/3\(6\)CR](#)

Le Linee Guida del Garante Privacy italiano sui cookies ed altri strumenti di tracciamento del 10 giugno 2021

[2021/4\(3\)CR](#)

Le rilevanti modifiche al Codice Privacy introdotte dal 'Decreto Capienze' del 7 ottobre 2021 come convertito in legge con modifiche ad opera della legge 3 dicembre 2021 n. 205

[2022/1\(9\)CR](#)

La decisione del 13 gennaio 2022 del garante privacy austriaco sul trasferimento di dati personali negli USA da parte di Google Analytics

[2022/1\(10\)CR](#)

La decisione del 10 febbraio 2022 del garante privacy francese sul trasferimento di dati personali negli USA da parte di Google Analytics

[2022/3\(8\)CR](#)

NOYB denuncia Google alla CNIL per l'invio di e-mail pubblicitarie non richieste senza consenso degli utenti

[2022/3\(9\)CR](#)

Il Garante privacy esprime parere negativo sullo schema di decreto sull'Ecosistema Dati Sanitari

[2022/4\(8\)CR](#)

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

**VALENTINO RAVAGNANI (VR)**

[2021/4\(8\)VR](#)

L'ordinanza del 16 settembre 2021 del Garante Privacy a proposito del sistema software di supervisione degli studenti "Respondus" impiegato dall'Università Bocconi di Milano per le prove scritte di esame

[2022/1\(11\)VR](#)

La decisione del 2 febbraio 2022 del garante privacy belga sul Real Time Bidding e le attività di online advertising a proposito del Quadro di Trasparenza e Consenso elaborato e gestito da IAB Europe

[2022/2\(7\)VR](#)

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*

[2022/3\(4\)VR](#)

La proposta di Regolamento UE sui requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali (c.d. Cyber Resilience Act)

[2022/4\(2\)VR](#)

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

[2022/4\(12\)VR](#)

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

**FEDERICO RUGGERI (FR)**

[2020/2\(1\)FR](#)

La Comunicazione della Commissione europea COM(2020) 66 final “Una strategia europea per i dati”

[2021/1\(7\)FR](#)

Regolamento P2B e nuove funzioni delle Autorità indipendenti alla luce della Legge di Bilancio 2021

**SUSANNA SANDULLI (SS)**

[2021/4\(11\)SS](#)

Le classi di rischio dei ‘Software As Medical Device’ (SAMDs) alla data di piena applicazione del Regolamento 2017/745 UE sui dispositivi medicali

**CHIARA SARTORIS (CS)**

[2021/3\(2\)SO-CS](#)

La Corte di Cassazione subordina la validità del consenso al trattamento dei dati personali alla trasparenza dell’algoritmo che governa il servizio per il quale il consenso è prestato (ordinanza 14381 del 25 maggio 2021 a proposito di un servizio di calcolo del c.d rating reputazionale)

**MARTINA SCOPSI (MS)**

[2020/4\(2\)MS](#)

La proposta della Commissione europea del 24 settembre 2020 avente ad oggetto l’emanazione di un Regolamento Europeo sui Mercati di Cripto-attività

**EMANUELE STABILE (ES)**

[2021/4\(9\)ES](#)

L’apertura della prima finestra temporale sulla sandbox regolamentare per i progetti fintech di cui al Decreto del MEF n. 100 del 30 aprile 2021

[2022/1\(7\)ES](#)

Il Decreto del Ministero dell’economia e delle finanze del 13 gennaio 2022 sull’iscrizione alla sezione speciale del registro dei cambiavalute da parte dei prestatori di servizi relativi all’utilizzo di valuta virtuale e di portafoglio digitale

[2022/2\(8\)ES](#)

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

[2022/2\(9\)ES](#)

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

[2022/3\(6\)ES](#)

Gli ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection

[2022/4\(3\)ES](#)

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

[2022/4\(13\)ES](#)

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

### **SARA TOMMASI (ST)**

[2021/1\(3\)ST](#)

Verso il *Digital Services Act*: la Proposta di Regolamento sul “mercato unico dei servizi digitali” del 15.12.2020

[2022/1\(5\)ST](#)

La proposta di Dichiarazione europea sui diritti e i principi digitali per il decennio digitale COM(2022) 28 final del 26 gennaio 2022

[2022/4\(1\)ST](#)

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

[2022/4\(7\)ST](#)

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

### **CARMINE ANDREA TROVATO (CAT)**

[2022/4\(9\)CAT](#)

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

### **LAVINIA VIZZONI (LV)**

[2021/3\(5\)LV](#)

Le Linee Guida EDPB del 7 luglio 2021 sugli assistenti vocali virtuali

## INDICE ANALITICO

### A

**Abusivismo (reato ex art. 166 TUF):** [2022/4\(13\)ES](#)

**Abuso di dipendenza economica:** [2022/4\(4\)SO](#)

**Abuso di mercato (mercati delle cripto-attività):** [2022/2\(3\)AF](#)

**Abuso di informazioni privilegiate (mercati delle cripto-attività):** [2022/2\(3\)AF](#)

**Abuso di posizione dominante:** [2020/4\(6\)DPDM](#); [2021/2\(9\)DPDM](#)

**Accesso a reti o a banche di dati (diritto d'autore):** [2022/1\(1\)EB](#)

**Ads Personalization (Google):** [2022/4\(18\)RMo](#)

#### **AGCM:**

- *Caso PS11112 - FACEBOOK-CONDIVISIONE DATI CON TERZI: provvedimento n. 27432 del 29.11.2018 di contestazione di pratiche commerciali scorrette a Facebook (claim "Facebook è gratis e lo sarà sempre"):* [2020/1\(4\)MG](#)
- [2021/1\(7\)FR](#)
- *Caso PS11150 – ICLOUD: provvedimento n. 88529 del 9.11.2021 dell'AGCM di contestazione di pratiche commerciali scorrette a carico di Apple:* [2022/4\(19\)AM-GD](#)
- *Caso PS11147: provvedimento n. 29890 del 16.11.2021 dell'AGCM di contestazione di pratiche commerciali scorrette a carico di Google:* [2022/4\(19\)AM-GD](#)

**AGCOM:** [2021/1\(7\)FR](#); [2022/1\(1\)EB](#)

**AGEA:** [2022/4\(15\)FDA](#)

**Agenzia per le Erogazioni in Agricoltura** (v. AGEA)

**Agenzia per l'Italia Digitale** (v. AGID)

**Agenzia dell'Unione europea per la cibersicurezza** (v. ENISA)

**AGID:** [2020/1\(8\)EWDM](#)

**AIA** (v. AI Act)

**AI Act:** [2021/2\(1\)SO](#); [2021/3\(3\)CR](#); [2022/2\(8\)ES](#)

**AI** (v. Intelligenza Artificiale)

**AI Liability:** [2020/2\(3\)SO](#); [2020/4\(1\)SG](#)

**AI Liability Directive:** [2022/3\(1\)TDMCDV](#)

**Algorithm Charter of New Zealand:** [2020/3\(7\)EMI](#)

**Altruismo dei dati:** [2021/4\(4\)RA](#); [2022/2\(1\)RA](#)

**Amazon:** [2020/4\(6\)DPDM](#)

**Ambiente digitale (diritto d'autore):** [2022/1\(1\)EB](#)

**Ambiente digitale sicuro e protetto:** [2022/4\(5\)RA](#)

**Ambito di applicazione territoriale GDPR (criterio del targeting):** [2022/1\(8\)GDI](#)

**Amplificazione:** [2022/1\(6\)SO](#)

**Amplificazione e pubblicità politica:** [2022/1\(6\)SO](#)

**Anonimizzazione dei dati:** [2022/4\(14\)EB](#)

**Antitrust Italiana** (v. AGCM)

**API:** [2021/2\(10\)EMI](#)

**Apple:** [2021/1\(9\)CM](#); [2021/2\(5\)FP](#); [2021/2\(9\)DPDM](#); [2022/4\(19\)AM-GD](#)

**Apple ecosystem:** [2021/2\(5\)FP](#)

**App Store:** [2021/2\(9\)DPDM](#)

**Application Programming Interface** (v. API)

**Applicazioni di messagistica:** [2021/2\(5\)FP](#)

**Applicazioni circolari intelligenti:** [2021/1\(2\)GC](#)

**Applicazioni di musica in streaming:** [2021/2\(9\)DPDM](#)

**Applicazione IO:** [2021/4\(3\)CR](#)

**Artificial Intelligence** (v. Intelligenza Artificiale)

**Artificial Intelligence Act** (v. AI Act)

**Assistenti virtuali:** [2021/2\(1\)SO](#); [2021/3\(5\)LV](#)

**Assistenti vocali virtuali:** [2021/3\(5\)LV](#)

**Atti amministrativi generali (base giuridica del trattamento dei dati personali):**  
[2021/4\(3\)CR](#)

**Attività amministrativa e impiego di procedure informatizzate:** [2021/4\(7\)FDA](#);  
[2022/1\(13\)FDA](#); [2022/4\(15\)FDA](#)

**Austria:** [2022/1\(9\)CR](#)

**Automated decision making** (v. Decisioni basate unicamente su trattamenti automatizzati di dati personali)

**Autorità bancaria europea** (v. EBA)

**Autorità europea degli strumenti finanziari e dei mercati** (v. ESMA)

**Autorità garante della concorrenza e mercato** (v. AGCM)

**Autorità indipendenti:** [2021/1\(7\)FR](#)

**Autorità per le garanzie nelle comunicazioni** (v. AGCOM)

**Autorizzazione per i fornitori di servizi per le crypto-attività:** [2022/2\(3\)AF](#); [2022/1\(7\)ES](#)

**Assemblea societaria:** [2020/1\(2\)MP](#)

**Avvocato Generale presso la CGUE:** [2020/3\(2\)FB](#); [2022/2\(4\)FG](#)

## **B**

**Banca Centrale Europea** (v. BCE)

**Banca d'Italia:** [2021/2\(7\)EP](#); [2021/4\(9\)ES](#); [2022/2\(9\)ES](#)

**Banche Centrali dei Paesi G7:** [2021/4\(10\)AF](#)

**Banche di dati (diritto d'autore):** [2022/1\(1\)EB](#)

**Banche di dati di test (protezione dei dati personali):** [2022/4\(8\)CR](#)

**Basi giuridiche del trattamento dei dati personali:** [2021/4\(3\)CR](#); [2022/3\(8\)CR](#)

**BCE:** [2020/2\(8\)EP](#); [2021/3\(7\)AF](#); [2022/2\(8\)ES](#)

**B2C and B2B data sharing:** [2021/4\(4\)RA](#)

**Belgio:** [2022/1\(11\)VR](#); [2022/4\(9\)CAT](#)

**Beni digitali e Classe 9 della Classificazione di Nizza (marchi):** [2022/4\(16\)FG](#)

**Best efforts e responsabilità dei prestatori di servizi di condivisione di contenuti online (diritto d'autore):** [2022/1\(1\)EB](#); [2022/2\(4\)FG](#)

**Bias:** [2020/2\(2\)CR](#)

**Big Data:** [2021/2\(5\)FP](#)

**Bitcoin:** [2021/3\(8\)FP](#); [2022/4\(13\)ES](#)

**Blockchain** (v. Tecnologie a registro distribuito)

**Blogs:** [2021/1\(8\)CR](#); [2022/1\(8\)GDI](#);

**Brevetti per invenzioni industriali:** [2021/4\(6\)FG](#); [2022/2\(5\)SO](#)

## **C**

**CAD:** [2021/1\(8\)CR](#)

**Cancellazione dei dati personali:** [2022/4\(9\)CAT](#)

**Carta dei diritti fondamentali dell'Unione Europea** (v. CDFUE)

**Carta derechos digitales del Gobierno spagnolo:** [2021/3\(1\)DI](#)

**Carta di Nizza** (v. Carta dei diritti fondamentali dell'Unione Europea)

**Caso Marx (Clearview AI, Germania):** [2021/1\(8\)CR](#); [2022/1\(8\)GDI](#)

**Cassazione** (v. Corte di Cassazione)

**Categorizzazione biometrica:** [2021/1\(8\)CR](#); [2021/2\(1\)SO](#); [2022/1\(8\)GDI](#)

**CBDC retail (Retail Central Bank Digital Currency):** [2021/4\(10\)AF](#)

**CBDC wholesale:** [2021/4\(10\)AF](#)

**CBDC account:** [2021/4\(10\)AF](#)

**CDFUE:** [2022/1\(5\)ST](#); [2022/4\(12\)VR](#)

**CDSMD Copyright in Digital Single Market Directive** (v. Direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale)

**CGUE :**

- Sentenza “Schrems II” della CGUE del 16.7.2020 sul Privacy Shield con gli USA e sulle clausole contrattuali tipo: [2020/3\(1\)CR](#)
- Sentenza della CGUE del 15.9.2020 nelle (C-807/18 e C-39/19 riunite) sul principio di «neutralità di Internet» ai sensi del regolamento (UE) 2015/2120: [2020/4\(3\)MP](#)
- Sentenza della CGUE del 6.10.2021 (C-13/20) sul diritto di decompilazione del software (il caso Top System): [2021/4\(5\)EMI](#)
- Sentenza della CGUE del 25.11.2021, StWL Städtische Werke Lauf a.d Pegnitz (C-102/20) su email e inbox advertising: [2022/3\(8\)CR](#)
- Sentenza della CGUE del 26.4.2022 su ricorso della Polonia avverso alcune disposizioni dell'art. 17 della Direttiva (UE) 2019/790 sul copyright nel mercato unico digitale (C-401/19): [2022/2\(4\)FG](#)
- Sentenza della CGUE del 20.10.2022 nella causa C 77/21 sui principi di limitazione delle finalità e di limitazione della conservazione ex art. 5 lett. b) ed e) GDPR: [2022/4\(8\)CR](#)
- Sentenza della CGUE del 27.10.2022 nella causa C-129/21 Proximus (Annuaire électroniques publics) sulle misure da adottarsi da parte del titolare del trattamento di dati personali per informare i motori di ricerca in Internet di una richiesta di cancellazione rivoltagli dall'interessato: [2022/4\(9\)CAT](#)

**Chatbot:** [2021/2\(1\)SO](#); [2021/3\(5\)LV](#)

**Ciclofattorini:** [2021/3\(9\)AN](#); [2022/2\(12\)VP](#)

**Cina (Repubblica Popolare Cinese):** [2020/4\(4\)CM](#); [2021/3\(4\)CM](#); [2021/4\(13\)CM](#)

**Classe 9 della Classificazione di Nizza (domande di marchio dell'Unione Europea):**

[2022/4\(16\)FG](#)

**Classi di rischio (software come dispositivi medici):** [2021/4\(11\)SS](#)

**Classificazione di Nizza (domande di marchio dell'UE):** [2022/4\(16\)FG](#)

**Clausole contrattuali abusive relative all'accesso ai dati e al relativo utilizzo:**

[2022/3\(3\)RA](#)

**Clausole contrattuali tipo per trasferimento dati personali all'estero:** [2020/3\(1\)CR](#)

**Clearview AI:** [2021/1\(8\)CR](#); [2022/1\(8\)GDI](#)

**CNIL** (v. Garante francese per la protezione dei dati personali)

**Code of Practice on Disinformation:** [2021/1\(1\)DPDM](#); [2022/4\(6\)DI](#)

**Codice dell'Amministrazione Digitale** (v. CAD)

**Codice dei beni culturali e del paesaggio (D.lgs. 22 gennaio 2004, n. 42, c.d. Codice Urbani):** [2022/1\(1\)EB](#)

**Codice di buone pratiche sulla disinformazione:** [2021/1\(1\)DPDM](#); [2022/4\(6\)DI](#)

**Codice del consumo:** [2021/4\(1\)FBc](#)

**Codice europeo delle comunicazioni elettroniche** (v. Direttiva (UE) 2018/1972 istitutiva del Codice europeo delle comunicazioni elettroniche)

**Codice in materia di protezione dei dati personali** (v. Codice privacy)

**Codice privacy:** [2021/1\(9\)CM](#); [2021/3\(2\)SO-CS](#); [2021/3\(6\)CR](#); [2021/3\(9\)AN](#); [2021/4\(3\)CR](#); [2022/1\(12\)FG](#); [2022/4\(14\)EB](#)

**Codice sorgente (programmi per elaboratori):** [2021/4\(5\)EMI](#)

**Codice Urbani** (v. Codice dei beni culturali e del paesaggio)

**Comitato Europeo per l'innovazione in materia di dati:** [2021/4\(4\)RA](#)

**Comitato Europeo per la protezione dei dati personali** (v. EDPB)

**Comitato europeo per il rischio sistemico** (v. ESRB)

**Comitato per l'Europa interoperabile:** [2022/4\(10\)FDA](#)

**Comitato dei rappresentanti permanenti** (v. COREPER)

**Commercio elettronico:** [2020/3\(2\)FB](#); [2022/4\(1\)ST](#)

**Commission Nationale de l'Informatique et des Libertés (CNIL)** (v. Garante francese per la protezione dei dati personali)

**Commissione Europea:** [2020/4\(2\)MS](#); [2020/4\(6\)DPDM](#); [2021/1\(1\)DPDM](#); [2021/1\(3\)ST](#); [2021/1\(4\)EMI](#); [2021/2\(9\)DPDM](#); [2021/2\(1\)SO](#); [2022/1\(4\)SO](#); [2022/3\(1\)TDMCDV](#); [2022/3\(2\)TDMCDV](#); [2022/3\(3\)RA](#); [2022/4\(3\)ES](#); [2022/4\(5\)RA](#); [2022/4\(10\)FDA](#)

Commissione JURI del Parlamento Europeo: [2020/2\(2\)CR](#)

Commissione nazionale società e borsa (Consob): [2021/2\(7\)EP](#); [2021/4\(9\)ES](#)

Computer-generated works (diritto d'autore): [2022/2\(5\)SO](#)

Comune di Arezzo: [2022/4\(12\)VR](#)

Comune di Lecce: [2022/4\(12\)VR](#)

Comunicazione della Commissione europea COM(2020) 66 final “Una strategia europea per i dati”: [2020/2\(1\)FR](#)

Comunicazione della Commissione europea “Plasmare il futuro digitale dell’Europa”: [2022/4\(2\)VR](#)

Comunicazione e diffusione di dati personali: [2021/4\(3\)CR](#)

Concorrenza sleale: [2022/4\(16\)FG](#)

Condivisione dei dati: [2021/4\(4\)RA](#)

Consenso al trattamento dei dati personali (consenso privacy): [2021/3\(2\)SO-CS](#); [2022/3\(8\)CR](#); [2022/4\(8\)CR](#); [2022/4\(9\)CAT](#)

Conservazione dei dati: [2022/4\(8\)CR](#)

Consiglio dell’Unione Europea: [2022/2\(3\)AF](#); [2022/3\(3\)RA](#); [2022/4\(5\)RA](#)

Consiglio di Stato

- Sentenza n. 2631 del 29.03.2021 nel caso Facebook (gratuità del servizio e divieto di pratiche commerciali scorrette): [2021/2\(8\)MG](#)

Consob (Commissione nazionale società e borsa): [2021/2\(7\)EP](#); [2021/4\(9\)ES](#)

Consumatori (v. Diritto del consumo)

Content moderation/supervision: [2020/2\(6\)DI](#); [2020/3\(2\)FB](#); [2021/2\(4\)FP](#)

Contenzioso online: [2021/3\(10\)CM](#)

Contesto transfrontaliero (diritto d'autore): [2022/1\(1\)EB](#)

Contestualizzazione dei dati personali: [2022/4\(14\)EB](#)

Controllo sui contenuti: [2020/2\(6\)DI](#); [2020/3\(2\)FB](#); [2021/2\(4\)FP](#); [2022/1\(1\)EB](#); [2022/4\(7\)ST](#)

Contenuti digitali associati agli NFTs (Non-Fungible Tokens): [2022/4\(16\)FG](#)

Contenuti offensivi: [2020/2\(6\)DI](#); [2021/2\(4\)FP](#)

Cookies e altri strumenti di tracciamento: [2020/2\(5\)EMI](#); [2021/3\(6\)CR](#); [2022/4\(11\)SO](#)

Cookie wall: [2020/2\(5\)EMI](#); [2022/4\(11\)SO](#)

Cooperazione transfrontaliera tra le amministrazioni degli Stati membri dell’UE: [2022/4\(10\)FDA](#)

**Copie cache:** [2022/1\(12\)FG](#)

**Copyright** (v. Diritto d'autore)

**Copyright in Digital Single Market Directive** (v. Direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale)

**COREPER:** [2022/4\(5\)RA](#)

**Coronavirus:** [2020/1\(1\)RM](#)

**Corte di Appello dell'Inghilterra e del Galles**

- Civil Division, sentenza del 21.9.2021 sulla capacità di inventore del sistema di IA 'DABUS' (Thaler v Comptroller General of Patents Trade Marks and Designs [2021] EWCA Civ 1374): [2021/4\(6\)FG](#)

**Corte di Appello di Parigi:** [2020/4\(7\)LC](#)

**Corte di Cassazione**

- Sentenza Sez. 2 Penale n. 26807/2020 in materia di vendite di criptovalute e all'equiparazione delle criptovalute a prodotti finanziari: [2022/4\(13\)ES](#)
- Ordinanza 14381 del 24.5.2021 su servizio di rating reputazionale e trasparenza dell'algoritmo (caso Mevaluate): [2021/3\(2\)SO-CS](#)
- Sentenza Sez. 1 Civile n. 3952 del 8.2.2022 sul diritto all'oblio e le copie cache (Yahoo!): [2022/1\(12\)FG](#)
- Sentenza Sez. 2 Penale 44378 del 26.10.2022 sulla qualificazione della moneta virtuale a proposito di un sequestro penale preventivo di wallet contenente bitcoin e del reato di esercizio abusivo dell'attività finanziaria: [2022/4\(13\)ES](#)
- Ordinanza Sez. 1 Civile 34658 del 24.11.2022 sul diritto all'oblio (regime Codice privacy anteriore al GDPR) (global delisting Google): [2022/4\(14\)EB](#)

**Corte di Giustizia dell'Unione Europea** (v. CGUE)

**Corte Suprema degli Stati Uniti d'America**

- Opinion del 5 aprile 2021 nella causa Google LLC v. Oracle (Certiorari to the United States Court Of Appeals for the Federal Circuit) in materia di API e diritto d'autore

**Costituzione italiana:** [2020/3\(3\)LC](#); [2020/3\(4\)FP](#); [2022/4\(14\)EB](#)

**Costituzione francese:** [2020/1\(6\)DI](#)

**Covid-19 (epidemia Sars Covid):** [2020/2\(7\)MP](#); [2021/4\(8\)VR](#)

**Cripto-attività:** [2020/1\(3\)EMI](#); [2020/4\(2\)MS](#); [2021/2\(7\)EP](#); [2022/2\(3\)AF](#); [2022/4\(13\)ES](#)

**Cripto-valute:** [2021/4\(10\)AF](#); [2021/4\(12\)BC](#); [2022/1\(7\)ES](#); [2022/2\(2\)BC](#); [2022/4\(13\)ES](#)

**Crypto-assets** (v. Cripto-attività)

Crypto-currencies (v. Cripto-valute)

Crypto-lending: [2022/2\(3\)AF](#)

Cyber Resilience Act: [2022/3\(4\)VR](#)

Cybersicurezza: [2022/3\(4\)VR](#); [2022/4\(3\)ES](#)

## D

DAOs : [2021/4\(12\)BC](#)

DABUS: [2021/4\(6\)FG](#)

Dark patterns: [2022/4\(1\)ST](#)

Data Act: [2022/1\(4\)SO](#); [2022/3\(3\)RA](#)

Data altruism (v. Altruismo dei dati)

Data economy: [2020/2\(1\)FR](#);

Data governance: [2020/2\(1\)FR](#); [2021/4\(4\)RA](#); [2022/2\(1\)RA](#)

Data Governance Act DGA: [2021/4\(4\)RA](#); [2022/2\(1\)RA](#)

Data intermediation services (v. Servizi di intermediazione dei dati)

Data monetization (v. Monetizzazione dei dati personali)

Data Protection (v. Dati personali)

Data Protection Supervisor (v. European Data Protection Supervisor)

Data retention (v. Conservazione dei dati personali)

Data sharing (v. Condivisione dei dati)

Datenschutzbehörde (DSB) (v. Garante austriaco per la protezione dei dati personali)

Dati biometrici: [2021/4\(8\)VR](#); [2022/1\(8\)GDI](#); [2022/4\(12\)VR](#)

Dati di addestramento: [2021/2\(1\)SO](#)

Dati di convalida: [2021/2\(1\)SO](#)

Dati di geolocalizzazione: [2022/4\(18\)RMo](#)

Dati di prova: [2021/2\(1\)SO](#)

Dati personali: [2020/3\(1\)CR](#); [2020/4\(4\)CM](#); [2021/3\(9\)AN](#); [2021/4\(3\)CR](#); [2021/4\(4\)RA](#);  
[2021/4\(8\)VR](#); [2021/4\(13\)CM](#); [2022/1\(11\)VR](#); [2022/1\(12\)FG](#); [2022/2\(9\)ES](#); [2022/3\(3\)RA](#);  
[2022/4\(8\)CR](#); [2022/4\(9\)CAT](#); [2022/4\(12\)VR](#); [2022/4\(18\)RMo](#); [2022/4\(11\)SO](#);  
[2022/4\(14\)EB](#)

Dati personali sensibili ex art. 9 GDPR: [2021/4\(3\)CR](#); [2022/1\(6\)SO](#); [2022/1\(8\)GDI](#);  
[2022/2\(10\)AAM](#)

**Dati Sanitari:** [2022/3\(9\)CR](#)

**DCD** (v. Direttiva (UE) 2019/770 sui contratti di fornitura di contenuti e servizi digitali)

**Decentralized Autonomous Organizations** (v. DAOs)

**Decentralized Finance (DeFi):** [2022/2\(3\)AF](#)

**Decisioni automatizzate** (v. Decisioni basate unicamente su trattamenti automatizzati di dati personali)

**Decisioni basate unicamente su trattamenti automatizzati di dati personali:**

[2021/4\(7\)FDA](#); [2022/1\(8\)GDI](#); [2022/1\(13\)FDA](#); [2022/4\(15\)FDA](#)

**Decompilazione:** [2021/4\(5\)EMI](#)

**Decreto Legislativo 231/2007 del 21.11.2007** attuativo della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione: [2022/4\(13\)ES](#)

**Decreto Legislativo 125/2019 del 4.10.2019** recante modifiche ed integrazioni ai decreti legislativi 25 maggio 2017, n. 90 e n. 92, recanti attuazione della direttiva (UE) 2015/849, nonché attuazione della direttiva (UE) 2018/843 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE: [2022/4\(13\)ES](#)

**Decreto Legge ‘Capienze’ n. 139 del 7.10.2021** e legge di conversione n. 205 del 3.12.2021: [2021/4\(3\)CR](#); [2022/4\(12\)VR](#)

**Decreto Legislativo 177/2021 del 5.11.2021** attuativo della Direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale: [2022/1\(1\)EB](#)

**Decreto Legislativo 200/2021 del 8.11.2021** attuativo della Direttiva (UE) 2019/1024 (direttiva Open Data): [2022/1\(2\)RA](#)

**Decreto Legislativo 207/2021 del 8.11.2021** attuativo della Direttiva (UE) 2018/1972 (Codice europeo delle comunicazioni elettroniche): [2022/1\(3\)EMI](#)

**Decreto MEF n. 100 del 30.4.2021** sulla sperimentazione Fintech: [2021/4\(9\)ES](#)

**Decreto MEF del 13.1.2022 sull'iscrizione alla sezione speciale del registro dei cambiavalute da parte dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale:** [2022/1\(7\)ES](#)

**Deep fake:** [2021/2\(1\)SO](#); [2022/4\(6\)DI](#)

**DeFi** (v. Decentralized Finance)

**Deindicizzazione (diritto all'oblio):** [2022/1\(12\)FG](#); [2022/4\(14\)EB](#)

**Deliveroo:** [2021/3\(9\)AN](#); [2022/2\(12\)VP](#)

**Democrazia:** [2021/1\(1\)DPDM](#)

**De-selezione del consenso privacy:** [2022/4\(19\)AM-GD](#)

**Device for the Autonomous Bootstrapping of Unified Sentience (sistema di IA) (v. DABUS)**

**DGA** (v. Data Governance Act)

**Diffamazione on line:** [2020/2\(6\)DI](#)

**Digital Compass 2030:** [2022/4\(5\)RA](#)

**Digital Content Directive** (v. Direttiva (UE) 2019/770 sui contratti di fornitura di contenuti e servizi digitali)

**Digital currencies:** [2021/4\(10\)AF](#); [2022/1\(7\)ES](#)

**Digital Markets Act:** [2021/1\(4\)EMI](#); [2022/4\(2\)VR](#)

**Digital payments:** [2022/1\(7\)ES](#)

**Digital Services Act :** [2021/1\(3\)ST](#); [2021/1\(5\)RMo](#); [2022/4\(1\)ST](#)

**Digital Single Market** (v. Mercato unico digitale)

**Dignità:** [2022/4\(14\)EB](#)

**Direttiva sul Commercio Elettronico 2001/31/CE:** [2020/3\(2\)FB](#); [2022/4\(1\)ST](#)

**Direttiva ePrivacy 2002/58/CE:** [2021/3\(6\)CR](#); [2021/4\(4\)RA](#); [2022/3\(8\)CR](#); [2022/4\(9\)CAT](#); [2022/4\(11\)SO](#)

**Direttiva Infosoc 2011/29/CE:** [2020/3\(2\)FB](#)

**Direttiva Law Enforcement (UE) 2016/680:** [2022/2\(7\)VR](#)

**Direttiva Open Data (UE) 2019/1024:** [2021/4\(4\)RA](#); [2022/1\(2\)RA](#)

**Direttiva sulle Pratiche Commerciali Sleali 2005/29/CE:** [2020/1\(4\)MG](#); [2021/2\(8\)MG](#); [2022/4\(19\)AM-GD](#)

**Direttiva Software 91/250/CEE:** [2021/4\(5\)EMI](#)

**Direttiva Whistleblowing (UE) 2019/1937:** [2022/4\(2\)VR](#)

**Direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore** (v. Direttiva Software 91/250/CEE)

**Direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno** (v. Direttiva sul commercio elettronico 2001/31/CE)

**Direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione** (v. Direttiva Infosoc 2011/29/CE)

**Direttiva 2002/58/CE** relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (v. Direttiva ePrivacy 2002/58/CE)

**Direttiva 2005/29/CE** relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica le direttive 84/450/CEE, 97/7/CE, 98/27/CE e 2002/65/CE e il regolamento (CE) n. 2006/2004 (Direttiva sulle pratiche commerciali sleali 2005/29/CE)

**Direttiva (UE) 2016/680** 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 (v. Direttiva Law Enforcement (UE) 2016/680)

**Direttiva (UE) 2018/843** che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE: [2022/4\(13\)ES](#)

**Direttiva (UE) 2018/1972** istitutiva del Codice europeo delle comunicazioni elettroniche: [2022/1\(3\)EMI](#)

**Direttiva (UE) 2019/770** sui contratti di fornitura di contenuti e servizi digitali: [2021/4\(1\)FBc](#); [2021/4\(2\)FP](#)

**Direttiva (UE) 2019/771** su determinati aspetti dei contratti di vendita di beni di consumo: [2021/4\(1\)FBc](#)

**Direttiva (UE) 2019/790** sul diritto d'autore e sui diritti connessi nel mercato unico digitale: [2020/4\(7\)LC](#); [2022/1\(1\)EB](#); [2022/2\(4\)FG](#)

**Direttiva (UE) 2019/1024** relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (v. Direttiva Open Data (UE) 2019/1024)

**Direttiva (UE) 2019/1937** riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (v. Direttiva Whistleblowing (UE) 2019/1937)

**Direttiva (UE) 2020/1828/UE** relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE: [2022/4\(2\)VR](#)

**Diritti connessi (diritto d'autore):** [2020/4\(7\)LC](#); [2022/1\(1\)EB](#)

**Diritti di proprietà intellettuale:** [2020/2\(4\)LC](#); [2020/3\(1\)CR](#); [2020/4\(7\)LC](#); [2021/4\(4\)RA](#); [2021/4\(6\)FG](#); [2022/1\(1\)EB](#); [2022/2\(5\)SO](#)

**Diritti fondamentali:** [2021/3\(9\)AN](#); [2022/1\(5\)ST](#); [2022/1\(12\)FG](#); [2022/2\(4\)FG](#)  
[2022/3\(9\)CR](#); [2022/4\(7\)ST](#); [2022/4\(12\)VR](#); [2022/4\(5\)RA](#); [2022/4\(14\)EB](#)

**Diritto di acquisizione delle informazioni:** [2022/1\(12\)FG](#)

**Diritto all'accesso alla connettività digitale ad alta velocità a prezzi accessibili:**  
[2022/4\(5\)RA](#)

**Diritto d'autore:** [2020/3\(1\)CR](#); [2020/3\(2\)FB](#); [2020/4\(7\)LC](#); [2021/4\(5\)EMI](#); [2022/1\(1\)EB](#);  
[2022/2\(5\)SO](#); [2022/4\(16\)FG](#)

**Diritto alla cancellazione dei dati personali:** [2022/1\(12\)FG](#); [2022/4\(14\)EB](#);  
[2022/4\(9\)CAT](#)

**Diritto dei contratti:** [2021/4\(1\)FB](#); [2021/4\(2\)FP](#); [2021/4\(5\)EMI](#); [2021/4\(12\)BC](#);  
[2022/2\(6\)EMI](#); [2022/3\(6\)ES](#)

**Diritto dei consumatori** (v. Diritto del consumo)

**Diritto del consumo:** [2021/2\(8\)MG](#); [2021/4\(1\)FB](#); [2021/4\(2\)FP](#); [2022/3\(6\)ES](#);  
[2022/3\(2\)TDMCDV](#); [2022/4\(19\)AM-GD](#)

**Diritto alla cancellazione dei dati personali:** [2022/4\(9\)CAT](#)

**Diritto di cronaca:** [2022/4\(14\)EB](#)

**Diritto alla deindicizzazione (diritto all'oblio):** [2022/1\(12\)FG](#); [2022/4\(14\)EB](#)

**Diritto di diffusione delle informazioni:** [2022/1\(12\)FG](#)

**Diritto (dei lavoratori) alla disconnessione:** [2021/1\(6\)LC](#)

**Diritto di famiglia:** [2021/1\(9\)CM](#)

**Diritto alla formazione permanente per acquisire competenze digitali di base e avanzate:** [2022/4\(5\)RA](#)

**Diritto del lavoro:** [2021/3\(9\)AN](#); [2022/2\(12\)VP](#); [2022/4\(12\)VR](#)

**Diritto all'immagine:** [2022/4\(16\)FG](#)

**Diritto di informazione:** [2022/4\(14\)EB](#)

**Diritto a non essere trovati facilmente (diritto all'oblio):** [2022/1\(12\)FG](#); [2022/4\(14\)EB](#)

**Diritto all'oblio:** [2022/1\(12\)FG](#); [2022/4\(14\)EB](#)

**Diritto societario:** [2020/1\(2\)MP](#); [2021/4\(12\)BC](#)

**Diritto successorio:** [2021/1\(9\)CM](#)

**Disabilitazione dei contenuti online (diritto d'autore):** [2022/1\(1\)EB](#)

**Disponibilità dei dati:** [2022/4\(4\)SO](#)

**District Court of New Hampshire:** [2022/4\(17\)EMI](#)

**Distributed Ledger Technology** (v. Tecnologie a registro distribuito)

**Divieto di immissione sul mercato, messa in servizio e/o uso di determinati sistemi di Intelligenza Artificiale:** [2021/2\(1\)SO](#)

**DLT:** [2021/3\(10\)CM](#); [2021/4\(12\)BC](#); [2022/2\(2\)BC](#); [2022/3\(6\)ES](#); [2022/4\(17\)EMI](#)

**DMA** (v. Digital Markets Act)

**Dominio pubblico (diritto d'autore)** (v. Pubblico dominio (diritto d'autore))

**DORA:** [2022/4\(3\)ES](#)

**Droni:** [2020/1\(1\)RM](#);

**DSA** (v. Digital Services Act)

## **E**

**EBA:** [2022/2\(3\)AF](#); [2022/4\(3\)ES](#)

**Economia circolare:** [2022/3\(5\)EMI](#)

**Ecosistema Dati Sanitari:** [2022/3\(9\)CR](#)

**Editori online (diritto d'autore):** [2022/1\(1\)EB](#)

**EDPB:** [2020/2\(5\)EMI](#); [2021/3\(2\)SO-CS](#); [2022/2\(7\)VR](#); [2022/3\(7\)FG](#)

**EDPS:** [2021/1\(5\)RMo](#); [2021/2\(2\)CR](#); [2021/3\(2\)SO-CS](#); [2022/3\(7\)FG](#)

**EDS** (v. Ecosistema Dati Sanitari)

**Effetti di rete:** [2022/4\(4\)SO](#)

**EIOPA:** [2022/4\(3\)ES](#)

**Elenchi telefonici:** [2022/4\(9\)CAT](#)

**ELI:** [2022/1\(13\)FDA](#); [2022/3\(6\)ES](#)

**ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection- Council draft:** [2022/3\(6\)ES](#)

**El Salvador:** [2021/3\(8\)FP](#)

**Email pubblicitarie:** [2022/3\(8\)CR](#);

**Emittenti di cripto-attività non garantite e di stablecoin:** [2022/2\(3\)AF](#)

**Emotion reognition systems** (v. Sistemi IA di riconoscimento delle emozioni)

**Enac:** [2020/1\(1\)RM](#)

**England and Wales Court of Appeal (EWCA)** (v. Corte di Appello dell'Inghilterra e del Galles)

**ENISA:** [2022/3\(4\)VR](#)

**E-Privacy direttiva** (v. Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche)

**Equo compenso (diritto d'autore):** [2022/1\(1\)EB](#)

**Eredità digitale:** [2021/1\(9\)CM](#)

**Esercizio abusivo dell'attività finanziaria:** [2022/4\(13\)ES](#)

**ESMA:** [2022/2\(3\)AF](#); [2022/4\(3\)ES](#)

**ESRB:** [2022/4\(3\)ES](#)

**Estratto molto breve di pubblicazione di carattere giornalistico (diritto d'autore)** (v. Snippets (diritto d'autore))

**Estrazione (diritto d'autore):** [2022/1\(1\)EB](#)

**Estrazione di testo e di dati** (v. TDM)

**Etica ed Intelligenza Artificiale:** [2020/2\(2\)CR](#); [2020/4\(8\)SO](#)

**EU Interinstitutional declaration on digital rights and principles del 14.11.2022:**  
[2022/4\(5\)RA](#)

**EUIPO:** [2022/4\(16\)FG](#)

**EUIPO Draft Guidelines 2023:** [2022/4\(16\)FG](#)

**Euro digitale:** [2021/3\(7\)AF](#)

**Europa Interoperabile** (v. Interoperable Europe Act)

**European Banking Authority** (v. EBA)

**European Central Bank** (v. BCE)

**European Data Protection Supervisor** (v. EDPS)

**European Data Protection Board** (v. EDPB)

**European Democracy Action Plan del 03.12.2020:** [2021/1\(1\)DPDM](#)

**European Insurance and Occupational Pensions Authority** (v. EIOPA)

**European Law Institute** (v. ELI)

**European Network and Information Security Agency** (v. ENISA)

**European Union Agency for Cybersecurity** (v. ENISA)

**European Securities and Markets Authority** (v. ESMA)

**European Systemic Risk Board** (v. ESRB)

## **F**

**Facebook:** [2020/1\(4\)MG](#); [2020/3\(2\)FB](#); [2021/2\(8\)MG](#)

**Facial recognition** (v. Riconoscimento facciale)

**Fair use (diritto statunitense in materia di copyright):** [2021/2\(10\)EMI](#)

**Fascicolo sanitario elettronico:** [2020/4\(5\)CR](#); [2022/3\(9\)CR](#)

**Finalità del trattamento dei dati personali:** [2022/4\(8\)CR](#); [2022/4\(9\)CAT](#)

**Financial Stability Board** (v. FSB)

**Fintech:** [2021/4\(9\)ES](#)

**Fotografia semplice (diritto d'autore):** [2022/1\(1\)EB](#)

**Fornitori di servizi di intermediazione online:** [2021/1\(7\)FR](#)

**Fornitori di servizi per le cripto-attività:** [2022/2\(3\)AF](#)

**Francia:** [2020/1\(6\)DI](#); [2020/2\(6\)DI](#); [2020/4\(7\)LC](#); [2022/1\(10\)CR](#)

**FSB:** [2022/3\(11\)AF](#)

**FSE** (v. Fascicolo Sanitario Elettronico)

## **G**

**Garante della città di Amburgo per la protezione dei dati personali:** [2021/1\(8\)CR](#)

**Garante austriaco per la protezione dei dati personali (DSB):**

- decisione del 13.1.2022 sul trasferimento di dati personali negli USA per Google Analytics: [2022/1\(9\)CR](#)

**Garante belga per la protezione dei dati personali:**

- decisione del 2.2.2022 del Garante Privacy belga sul Real Time Bidding e le attività di online advertising a proposito del Quadro di Trasparenza e Consenso elaborato e gestito da IAB Europe: [2022/1\(11\)VR](#)
- decisione del 30.7.2022 del Garante privacy belga in materia di revoca del consenso privacy e diritto alla cancellazione dei dati personali (caso Proximus): [2022/4\(9\)CAT](#)

**Garante europeo per la protezione dei dati personali** (v. EDPS)

**Garante francese per la protezione dei dati personali**

- decisione del CNIL del 10.2.2022 sul trasferimento di dati personali negli USA per Google Analytics: [2022/1\(10\)CR](#)
- NOYB denuncia Google alla CNIL per l'invio di e-mail pubblicitarie non richieste senza consenso degli utenti: [2022/3\(8\)CR](#)

**Garante italiano per la protezione dei dati personali**

- provvedimento del GPDP del 25.2.2016 di parziale accoglimento in materia di diritto all'oblio (ingiunzione a Yahoo! di rimuovere gli URL e di cancellare copie cache): [2022/1\(12\)FG](#)
- provvedimento del GPDP n. 488 del 24.11.2016 su una piattaforma online di elaborazione di rating reputazionale (il caso Mevaluate): [2021/3\(2\)SO-CS](#)
- parere del GPDP del 29.4.2020 sull'applicazione volta al tracciamento dei contagi da Covid-19: [2020/2\(7\)MP](#)
- FAQ del GPDP dell'ottobre 2020 per la protezione dei dati personali sulla refertazione online: [2020/4\(5\)CR](#)
- parere del GPDP del 16.04.2021 sul sistema di riconoscimento facciale SARI Real Time da parte del Ministero dell'Interno: [2021/2\(3\)CR](#)
- Linee Guida del GPDP del 10.6.2021 sui cookies ed altri strumenti di tracciamento: [2021/3\(6\)CR](#)
- provvedimento del GPDP n. 285 del 22.7.2021 nei confronti di Deliveroo per il trattamento dei dati personali dei ciclo-fattorini: [2021/3\(9\)AN](#)
- decisione del GPDP del 16.9.2021 sul software di supervisione degli studenti "Respondus" impiegato dall'Università Bocconi di Milano per le prove scritte di esame: [2021/4\(8\)VR](#)
- decisione del GPDP del 10.2.2022 sul trattamento di dati biometrici da parte di Clearview AI: [2022/1\(8\)GDI](#)
- parere negativo del GPDP del 22.8.2022 sullo schema del Decreto Dati Sanitari: [2022/3\(9\)CR](#)
- comunicati del GPDP del 12.11.2022 del 21.10.2022 e del 18.10.2022 di avvio di istruttorie a carico di testate editoriali online per iniziative di cookie wall e monetizzazione di dati personali: [2022/4\(11\)SO](#)

**Garante ungherese per la protezione dei dati personali e la libertà di informazione:** [2022/4\(8\)CR](#)

**Gatekeepers:** [2021/2\(5\)FP](#); [2022/4\(2\)VR](#)

**GDPR:** [2020/3\(1\)CR](#); [2020/4\(5\)CR](#); [2021/1\(8\)CR](#); [2021/3\(2\)SO-CS](#); [2021/3\(6\)CR](#); [2021/3\(9\)AN](#); [2021/4\(3\)CR](#); [2021/4\(4\)RA](#); [2022/1\(9\)CR](#); [2022/1\(10\)CR](#); [2022/1\(12\)FG](#); [2022/2\(9\)ES](#); [2022/2\(10\)AAM](#); [2022/3\(9\)CR](#); [2022/4\(8\)CR](#); [2022/4\(12\)VR](#); [2022/4\(18\)RMo](#); [2022/4\(14\)EB](#)

**Gegevensbeschermingsautoriteit** (v. Garante belga per la protezione dei dati personali)

**Geolocalizzazione:** [2022/1\(8\)GDI](#)

**GEPD** (v. EDPS)

**Germania:** [2021/1\(8\)CR](#); [2021/4\(2\)FP](#)

**Gestione dei dati** (v. Data governance)

**Gig economy:** [2021/3\(9\)AN](#); [2022/2\(12\)VP](#)

**Global delisting (diritto all'oblio)** (v. Deindicizzazione da tutte le versioni, anche extraeuropee, di un motore di ricerca)

**Global removal (diritto all'oblio)** (v. Deindicizzazione da tutte le versioni, anche extraeuropee, di un motore di ricerca)

**Google:** [2020/3\(2\)FB](#); [2020/3\(6\)SG](#); [2020/4\(7\)LC](#); [2022/1\(9\)CR](#); [2022/1\(10\)CR](#); [2022/3\(8\)CR](#); [2022/4\(14\)EB](#); [2022/4\(18\)RMo](#); [2022/4\(19\)AM-GD](#)

**Google Analytics:** [2022/1\(9\)CR](#); [2022/1\(10\)CR](#)

**Google Drive:** [2022/4\(19\)AM-GD](#)

**Google ecosystem:** [2021/2\(5\)FP](#)

**Google Maps:** [2022/4\(19\)AM-GD](#)

**Google News:** [2020/4\(7\)LC](#)

**Google Payments:** [2022/4\(19\)AM-GD](#)

**Google Play Edicola:** [2022/4\(19\)AM-GD](#)

**Google Play Musica:** [2022/4\(19\)AM-GD](#)

**Google Play Store:** [2022/4\(19\)AM-GD](#)

**Google Search:** [2022/4\(19\)AM-GD](#)

**Google Store:** [2022/4\(19\)AM-GD](#)

**Google Traduttore:** [2022/4\(19\)AM-GD](#)

**Green Pass:** [2021/4\(3\)CR](#)

**GPDP** (v. Garante per la protezione dei dati personali italiano)

**Gruppo di esperti dell'Osservatorio sull'economia delle piattaforme online:** [2020/3\(4\)FP](#); [2021/2\(5\)FP](#)

## **H**

**Hate speech:** [2021/2\(4\)FP](#)

**Health Data:** [2020/4\(5\)CR](#)

**Hosting providers:** [2020/3\(2\)FB](#)

House Bill 20, Texas (HB): [2022/4\(7\)ST](#)

Howey test: [2022/4\(17\)EMI](#)

‘Human in the loop’: [2022/4\(15\)FDA](#)

## **I**

IA (v. Intelligenza Artificiale)

IAB Europe (Interactive Advertising Bureau Europe): [2022/1\(11\)VR](#)

ICO (v. Initial Coin Offering)

Identificazione biometrica: [2021/1\(8\)CR](#); [2021/2\(1\)SO](#); [2021/3\(3\)CR](#); [2021/4\(3\)CR](#);  
[2022/1\(8\)GDI](#)

Identità: [2022/4\(14\)EB](#)

Identità digitale: [2022/1\(8\)GDI](#); [2022/1\(12\)FG](#)

Impronta ambientale delle cripto-attività: [2022/2\(3\)AF](#)

Inbox advertising: [2022/3\(8\)CR](#)

Inclusione: [2022/4\(5\)RA](#)

Interactive Advertising Bureau Europe (IAB Europe): [2022/1\(11\)VR](#)

Indicizzazione (profilazione): [2022/1\(8\)GDI](#)

Initial Coin Offering: [2022/4\(13\)ES](#)

Intelligenza Artificiale: [2020/1\(6\)DI](#); [2020/2\(2\)CR](#); [2020/4\(1\)SG](#); [2020/4\(8\)SO](#);  
[2021/2\(1\)SO](#); [2021/4\(6\)FG](#); [2022/1\(8\)GDI](#); [2022/2\(5\)SO](#); [2022/2\(8\)ES](#);  
[2022/3\(1\)TDMCDV](#); [2022/3\(2\)TDMCDV](#); [2022/4\(12\)VR](#)

Internet of Things (v. IoT)

Infrastrutture di mercato basate sulla tecnologia a registro distribuito: [2022/2\(2\)BC](#)

Intermediazione dei dati: [2021/4\(4\)RA](#)

Internet delle cose (v. IoT)

Interoperable Europe Act: [2022/4\(10\)FDA](#)

Interoperabilità nel settore pubblico (v. Interoperable Europe Act)

Invenzioni e sistemi di IA: [2021/4\(6\)FG](#); [2022/2\(5\)SO](#)

Investimento finanziario: [2022/4\(13\)ES](#)

IoT: [2021/3\(5\)LV](#)

IPRs (v. Diritti di proprietà intellettuale)

Istituti di tutela del patrimonio culturale (diritto d'autore): [2022/1\(1\)EB](#)

Istituto per la vigilanza sulle assicurazioni (v. IVASS)

iTunes: [2022/4\(19\)AM-GD](#)

IVASS: [2021/4\(9\)ES](#)

## **J**

Java: [2021/2\(10\)EMI](#)

Juventus: [2022/4\(16\)FG](#)

## **K**

Know how: [2021/4\(4\)RA](#)

## **L**

LBRY, Inc.: [2022/4\(17\)EMI](#)

Legge n. 633/1941 (v. Legge sul diritto d'autore)

Legge sul diritto d'autore: [2021/4\(4\)RA](#); [2022/1\(1\)EB](#)

Legge di bilancio 2021: [2021/1\(7\)FR](#)

Legge sulla protezione delle informazioni personali della Repubblica Popolare  
Cinese del 20.8.2021 (v. PIPL)

Legge sulla subfornitura (Legge n. 192/1998): [2022/4\(4\)SO](#)

Ley Bitcoin della Repubblica di El Salvador dell'8.6.2021: [2021/3\(8\)FP](#)

Legge dello Stato del Wyoming sulle Decentralized Assets Organizations (DAOs) del  
21.4.2021: [2021/4\(12\)BC](#)

Libro Bianco della Commissione Europea del 19 febbraio 2020 sull'Intelligenza  
Artificiale: "Eccellenza e Fiducia": [2020/1\(5\)SO](#)

Licenza (diritto d'autore): [2022/1\(1\)EB](#)

Limitazione della conservazione (principio): [2022/4\(8\)CR](#)

Limitazione delle finalità (principio): [2022/4\(8\)CR](#)

Linee Guida del Garante Privacy del 10.6.2021 sui cookies ed altri strumenti di  
tracciamento: [2021/3\(6\)CR](#)

Linee Guide EDPB del 4.5.2020 sul consenso: [2020/2\(5\)EMI](#)

Linee Guida EDPB del 7.7.2021 sugli assistenti vocali virtuali: [2021/3\(5\)LV](#)

Linee Guide AGID per la sottoscrizione elettronica di documenti: [2020/1\(8\)EWDM](#)

Localbitcoin.com: [2022/4\(13\)ES](#)

Location data (v. Dati di geolocalizzazione)

Location History (Google): [2022/4\(18\)RMo](#)

## **M**

Machine inventor: [2021/4\(6\)FG](#); [2022/2\(5\)SO](#)

Manipolazione di mercato (mercati delle cripto-attività): [2022/2\(3\)AF](#)

Marchi (tutela): [2022/4\(16\)FG](#)

Marketplaces: [2021/2\(5\)FP](#)

Market power: [2021/2\(5\)FP](#)

Marx (caso): [2021/1\(8\)CR](#)

MDR (Medical Devices Regulation) (v. Regolamento (UE) 2017/745 relativo ai dispositivi medici)

MEF (Ministero dell'Economia e delle Finanze): [2021/4\(9\)ES](#)

Memorandum OSTP 2022 del 25.8.2022 sull'accesso ai risultati della ricerca scientifica negli Stati Uniti d'America: [2022/3\(10\)LC](#)

Mercati di cripto-attività: [2020/4\(2\)MS](#); [2022/2\(3\)AF](#)

Mercati equi e contendibili nel settore digitale: [2022/4\(2\)VR](#)

Mercato unico dei servizi digitali (DSA): [2021/1\(3\)ST](#); [2022/4\(1\)ST](#)

Mercato unico digitale (diritto d'autore): [2022/1\(1\)EB](#)

Meta: [2020/1\(4\)MG](#); [2020/3\(2\)FB](#)

Mevaluate (caso): [2021/3\(2\)SO-CS](#)

MiCAR Markets in Cripto-assets Regulation (v. Proposta di Regolamento sui mercati di cripto-attività 'MiCAR' COM(2020) 593 final-2020/0265(COD) del 24.9.2020)

Ministeri dell'Economia dei Paesi G7: [2021/4\(10\)AF](#)

Ministero dell'Economia e delle Finanze (MEF): [2021/4\(9\)ES](#); [2022/1\(7\)ES](#)

Ministero dell'Interno: [2021/2\(3\)CR](#)

Minori (protezione dei minori): [2021/2\(4\)FP](#)

**Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration** dello European Law Institute (ELI) del 3.3.2022: [2022/1\(13\)FDA](#)

**Moderazione dei contenuti:** [2022/4\(7\)ST](#)

**Moneta digitale / virtuale:** [2021/4\(10\)AF](#); [2022/1\(7\)ES](#); [2022/4\(13\)ES](#)

**Monetizzazione dei dati personali:** [2021/2\(8\)MG](#); [2021/4\(1\)FB](#)e; [2022/4\(19\)AM-GD](#); [2022/4\(11\)SO](#)

**Motori di ricerca online (Regolamento P2B):** [2021/1\(7\)FR](#)

**Motori di ricerca online (diritto all'oblio):** [2022/1\(12\)FG](#); [2022/4\(14\)EB](#)

## **N**

**Netchoice LLC:** [2022/4\(7\)ST](#)

**Network effect:** [2021/2\(5\)FP](#)

**Neuralink:** [2022/2\(10\)AAM](#)

**Neurodiritti:** [2022/2\(10\)AAM](#)

**Neuromarketing:** [2022/2\(10\)AAM](#)

**Neurorights** (v. Neurodiritti)

**Neuroscienze:** [2022/2\(10\)AAM](#)

**Neurotecnologie:** [2022/2\(10\)AAM](#)

**Neutralità di internet (principio):** [2020/4\(3\)MP](#)

**New Hampshire:** [2022/4\(17\)EMI](#)

**NFTs** (v. Non-Fungible Tokens)

**Non-Fungible Tokens (NFTs):** [2021/4\(12\)BC](#); [2022/2\(3\)AF](#); [2022/4\(16\)FG](#)

**Non Personal Data:** [2021/4\(4\)RA](#); [2022/3\(3\)RA](#)

**Noyb:** [2022/3\(8\)CR](#)

**Nuova Zelanda:** [2020/3\(7\)EMI](#)

## **O**

**OCSSP** (v. Prestatori di servizi di condivisione di contenuti online)

**Offerta al pubblico di prodotti finanziari:** [2022/4\(13\)ES](#)

**Office of Science and Technology Policy (OSTP)** del governo federale degli Stati Uniti d'America: [2022/2\(11\)AF](#)

**Online Content-Sharing Service Providers (OCSSP)** (v. Prestatori di servizi di condivisione di contenuti online)

**Online platforms** (v. Piattaforme online)

**Online targeting:** [2021/1\(5\)RMo](#);

**Open access (diritto d'autore):** [2022/1\(1\)EB](#)

**Open data:** [2021/4\(4\)RA](#); [2022/2\(11\)AF](#)

**Open Data Directive** (v. Direttiva Open Data (UE) 2019/1024)

**Open source:** [2021/2\(10\)EMI](#)

**Operatori fintech:** [2021/4\(9\)ES](#)

**Opere delle arti visive di dominio pubblico (diritto d'autore):** [2022/1\(1\)EB](#)

**Opere e altri materiali fuori commercio (diritto d'autore):** [2022/1\(1\)EB](#)

**Opinion power:** [2021/2\(5\)FP](#)

**Opt out (dati personali):** [2022/4\(9\)CAT](#)

**Oracle:** [2021/2\(10\)EMI](#)

**Organismi di ricerca (diritto d'autore):** [2022/1\(1\)EB](#)

**Organismi di gestione collettiva (diritto d'autore):** [2022/1\(1\)EB](#)

**Osservatorio sull'economia delle piattaforme online:** [2020/3\(4\)FP](#); [2021/2\(5\)FP](#)

**OSTP** (v. Office of Science and Technology Policy)

## **P**

**P2B** (v. Regolamento P2B (UE) 2019/1150)

**Pagamenti digitali:** [2021/4\(10\)AF](#)

**Payment Initiation Service Providers (PISP)**

**Paywall:** [2022/4\(11\)SO](#)

**Parere EDPS del 10.02.2021 sulla proposta del Digital Services Act:** [2021/1\(5\)RMo](#)

**Parere congiunto EDPB-EDPS n.4/2022 del 28.7.2022** sulla proposta di regolamento della Commissione Europea del 11.05.2022 che stabilisce norme per prevenire e combattere l'abuso sessuale dei minori: [2022/3\(7\)FG](#)

**Parere del Garante privacy italiano del 22.8.2022** sullo schema di decreto sull'Ecosistema Dati Sanitari: [2022/3\(9\)CR](#)

**Parlamento europeo:** [2020/4\(1\)SG](#); [2021/1\(2\)GC](#); [2021/1\(6\)LC](#); [2021/2\(4\)FP](#); [2022/2\(3\)AF](#); [2022/3\(3\)RA](#); [2022/4\(3\)ES](#); [2022/4\(5\)RA](#)

**Partecipazione allo spazio pubblico digitale:** [2022/4\(5\)RA](#)

**Passaporto dei prodotti digitale:** [2021/1\(2\)GC](#)

**Patrimonializzazione dei dati personali** (v. Monetizzazione dei dati personali)

**Patrimonio digitale:** [2021/1\(9\)CM](#)

**Patto per la sicurezza urbana tra Sindaco e Prefettura:** [2022/4\(12\)VR](#)

**Pennsylvania, USA:** [2022/4\(18\)RMo](#)

**Personalizzazione:** [2020/3\(6\)SG](#); [2022/4\(19\)AM-GD](#)

**Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo:** [2022/4\(3\)ES](#)

**Piattaforme online:** [2020/3\(1\)CR](#); [2020/3\(2\)FB](#); [2020/4\(6\)DPDM](#); [2021/1\(1\)DPDM](#); [2021/1\(7\)FR](#); [2021/2\(5\)FP](#); [2022/4\(4\)SO](#)

**Pirateria online:** [2021/2\(4\)FP](#)

**PIPL:** [2021/4\(13\)CM](#)

**Platform economy:** [2021/2\(5\)FP](#)

**PLD:** (v. Proposta COM(2022) 495 final del 28.9.2022 di Direttiva sulla responsabilità da prodotto)

**PNRR:** [2021/4\(3\)CR](#)

**Polonia:** [2022/2\(4\)FG](#)

**Portafoglio digitale:** [2022/1\(7\)ES](#)

**Pratiche commerciali scorrette:** [2021/2\(8\)MG](#); [2022/4\(19\)AM-GD](#)

**Pratiche di intelligenza artificiale vietate** (v. Divieto di immissione sul mercato, messa in servizio e/o uso di determinati sistemi di Intelligenza Artificiale)

**Prestatori di servizi di condivisione di contenuti online (diritto d'autore):** [2020/3\(2\)FB](#); [2022/1\(1\)EB](#); [2022/2\(4\)FG](#)

**Prestatori di servizi in crypto-attività:** [2022/2\(3\)AF](#); [2022/1\(7\)ES](#)

**Prestatori di servizi di portafoglio digitale:** [2022/4\(13\)ES](#)

**Prestatori di servizi relativi all'utilizzo di valuta virtuale:** [2022/4\(13\)ES](#)

**Primo Emendamento della Costituzione degli USA:** [2022/4\(7\)ST](#)

**Principio di accountability** (v. Principio di responsabilizzazione per il trattamento dei dati personali)

**Principio di limitazione della conservazione dei dati personali (art. 5 lett. e) GDPR):** [2022/4\(8\)CR](#)

**Principio di limitazione delle finalità (art. 5 lett. b) GDPR):** [2022/4\(8\)CR](#)

**Principio di responsabilizzazione ('accountability') per il trattamento dei dati personali (artt. 5 par. 2 e 24 GDPR):** [2022/4\(9\)CAT](#)

**Principio 'same activity, same risk, same regulation':** [2021/4\(10\)AF](#)

**Privacy by design/Privacy by default:** [2021/3\(9\)AN](#)

**Privacy Shield con gli USA:** [2020/3\(1\)CR](#); [2021/4\(8\)VR](#); [2022/1\(9\)CR](#); [2022/1\(10\)CR](#)

**Procedimento amministrativo:** [2021/4\(7\)FDA](#); [2022/1\(13\)FDA](#); [2022/4\(15\)FDA](#)

**Proctoring (sorveglianza durante gli esami online):** [2021/4\(8\)VR](#)

**Prodotti finanziari:** [2022/4\(13\)ES](#)

**Prodotti generatori di dati:** [2022/3\(3\)RA](#)

**Product Liability Directive** (v. Proposta COM(2022) 495 final del 28.9.2022 di Direttiva sulla responsabilità da prodotto)

**Profilazione:** [2021/1\(5\)RMo](#); [2021/1\(8\)CR](#); [2022/1\(6\)SO](#); [2022/1\(8\)GDI](#)

**Proposta COM(2020) 595 final del 24.9.2020 di Regolamento sulla resilienza operativa digitale nel settore finanziario** (v. DORA)

**Proposta COM(2020) 593 final-2020/0265(COD) del 24.9.2020 di Regolamento sui mercati di cripto-attività (MiCAR):** [2020/4\(2\)MS](#); [2022/2\(3\)AF](#)

**Proposta COM(2021) 206 final del 21.4.2021 di Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione sull'intelligenza artificiale** (v. AI Act)

**Proposta COM(2021) 731 final del 25.11.2021 di Regolamento relativo alla trasparenza e al targeting della pubblicità politica:** [2022/1\(6\)SO](#)

**Proposta COM(2022) 28 final del 26.1.2022 di Dichiarazione europea sui diritti e i principi digitali per il decennio digitale:** [2022/1\(5\)ST](#)

**Proposta COM(2022) 68 final del 23.2.2022 di Regolamento riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo** (v. Data Act)

**Proposta COM(2022) 209 final del 11.05.2022 di Regolamento che stabilisce norme per prevenire e combattere l'abuso sessuale dei minori:** [2022/3\(7\)FG](#)

**Proposta COM(2022) 454 final del 15.9.2022 di Regolamento sui requisiti orizzontali di cibersecurity per prodotti con elementi digitali che modifica il Regolamento (EU) 2019/1020 (regolamento sulla cibersecurity)** (v. Cyber Resilience Act)

**Proposta COM(2022) 495 final del 28.9.2022 di Direttiva sulla responsabilità da prodotto (Product Liability Directive): [2022/3\(2\)TDMCDV](#)**

**Proposta COM(2022) 496 final del 28.9.2022 di Direttiva sulla responsabilità da Intelligenza Artificiale (v. AI Liability Directive)**

**Proposta di Regolamento COM(2022) 720 final del 18.11.2022 sulla ‘Europa Interoperabile’ nel settore pubblico (v. Europe Interoperable Act)**

**Proposta dello U.S. Senate Banking Committee del 6.4.2022 di uno ‘US Stablecoin Trust Act’: [2022/2\(11\)AF](#)**

**Proprietà intellettuale (v. Diritti di proprietà intellettuale)**

**Proprietà intellettuale e Intelligenza Artificiale: [2020/2\(3\)SO](#)**

**Protezione dei consumatori (v. Diritto del consumo)**

**Protezione degli investitori in cripto-attività: [2022/2\(3\)AF](#)**

**Protezione dei minori: [2021/2\(4\)FP](#); [2022/3\(7\)FG](#)**

**Proximus NV: [2022/4\(9\)CAT](#)**

**Pubblicazioni elettroniche scaricabili e Classe 9 della Classificazione di Nizza (marchi): [2022/4\(16\)FG](#)**

**Pubblicazioni giornalistiche: [2022/1\(1\)EB](#)**

**Pubblicità mirata: [2021/1\(5\)RMo](#); [2022/1\(6\)SO](#); [2022/1\(11\)VR](#)**

**Pubblicità politica e amplificazione: [2022/1\(6\)SO](#)**

**Pubblico dominio (diritto d’autore): [2022/1\(1\)EB](#)**

**Public domain (v. Pubblico dominio (diritto d’autore))**

**Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs) del 13.10.2021: [2021/4\(10\)AF](#)**

**Punto di contatto unico (per il riutilizzo dei dati): [2021/4\(4\)RA](#)**

**P2B (v. Regolamento (UE) 2019/1150 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online (regolamento Platform to Business))**

## **Q**

## **R**

**Raccomandazione (sistemi di) (v. Recommender systems)**

**Rating reputazionale:** [2021/3\(2\)SO-CS](#)

**Real-time bidding:** [2022/1\(11\)VR](#)

**Reclamo contro la disabilitazione dei contenuti online (diritto d'autore):** [2022/1\(1\)EB](#)

**Recommender systems:** [2021/1\(3\)ST](#); [2021/1\(5\)RMo](#)

**Redimibilità alla pari degli stablecoin:** [2022/2\(3\)AF](#)

**Referti online:** [2020/4\(5\)CR](#)

**Regole sul contenzioso online dei Tribunali del Popolo della Repubblica popolare cinese del 28.5.2021:** [2021/3\(10\)CM](#)

**Registro distribuito** (v. Tecnologie a registro distribuito)

**Registro dei cambiavalute:** [2022/1\(7\)ES](#); [2022/4\(13\)ES](#)

**Registro dei fornitori di servizi di intermediazione dei dati:** [2021/4\(4\)RA](#); [2022/2\(1\)RA](#)

**Registro dei fornitori di servizi per cripto-attività non conformi:** [2022/2\(3\)AF](#)

**Registro degli operatori di comunicazione:** [2021/1\(7\)FR](#)

**Registro delle organizzazioni per l'altruismo dei dati:** [2021/4\(4\)RA](#); [2022/2\(1\)RA](#)

**Regno Unito:** [2020/1\(3\)EMI](#); [2022/2\(5\)SO](#)

**Regolamento DLT (UE) 2022/858:** [2022/2\(2\)BC](#); [2022/4\(3\)ES](#)

**Regolamento P2B (UE) 2019/1150:** [2021/1\(7\)FR](#)

**Regolamento (UE) 2015/2120 che stabilisce misure riguardanti l'accesso a un'Internet aperta:** [2020/4\(3\)MP](#)

**Regolamento (UE) 2017/745 relativo ai dispositivi medici**, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE (regolamento sui dispositivi medici, Medical Devices Regulation - MDR): [2021/4\(11\)SS](#)

**Regolamento (UE) 2019/1150 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online** (v. Regolamento P2B (UE) 2019/1150)

**Regolamento (UE) 2022/858 per un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito** (v. Regolamento DLT (UE) 2022/858)

**Regolamento (UE) 2022/868 relativo alla governance europea dei dati** (v. Data Governance Act)

**Regolamento (UE) 2022/1925 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive 2019/1937/UE e 2020/1828/UE (regolamento sui mercati digitali)** (v. Digital Markets Act)

**Regolamento (UE) 2022/2065 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE ('regolamento sui servizi digitali')** (v. Digital Services Act)

**Regno Unito:** [2020/1\(3\)EMI](#); [2021/4\(6\)FG](#); [2022/2\(5\)SO](#)

**Regolazione del mercato unico digitale:** [2020/2\(1\)FR](#)

**Relazione sull'impatto ambientale delle cripto-attività:** [2022/2\(3\)AF](#)

**Repubblica Popolare Cinese (Cina):** [2020/4\(4\)CM](#); [2021/3\(4\)CM](#); [2021/4\(13\)CM](#)

**Resilienza operativa digitale:** [2022/4\(3\)ES](#)

**Respondus (sistema software di supervisione degli studenti):** [2021/4\(8\)VR](#)

**Responsabilità da AI:** [2020/2\(3\)SO](#); [2022/3\(1\)TDMCDV](#)

**Responsabilità da prodotto:** [2021/4\(11\)SS](#); [2022/3\(2\)TDMCDV](#)

**Responsabilità delle piattaforme online:** [2020/3\(2\)FB](#); [2021/2\(4\)FP](#); [2022/1\(1\)EB](#)

**Responsabilità dei prestatori di servizi di condivisione di contenuti online (diritto d'autore):** [2020/3\(2\)FB](#); [2022/1\(1\)EB](#); [2022/2\(4\)FG](#)

**Retail Central Bank Digital Currency ("CBDC retail"):** [2021/4\(10\)AF](#)

**Revenge porn:** [2021/4\(3\)CR](#)

**Reverse engineering:** [2021/4\(5\)EMI](#)

**Revoca del consenso al trattamento dei dati personali:** [2022/4\(9\)CAT](#)

**Ricerca scientifica:** [2022/3\(10\)LC](#)

**Riconoscimento facciale:** [2021/2\(1\)SO](#); [2021/3\(3\)CR](#); [2021/4\(3\)CR](#); [2022/1\(8\)GDI](#); [2022/2\(7\)VR](#); [2022/4\(12\)VR](#)

**Riders** (v. Ciclofattorini)

**Right not to be found easily** (v. Diritto all'oblio; Deindicizzazione; Diritto a non essere trovati facilmente)

**Rimozione dei contenuti online (diritto d'autore):** [2022/1\(1\)EB](#)

**Rimozione degli URL (diritto all'oblio):** [2022/1\(12\)FG](#); [2022/4\(14\)EB](#)

**Riproduzione (diritto d'autore):** [2022/1\(1\)EB](#);

**Riserva di attività liquide per gli emittenti di stablecoin:** [2022/2\(3\)AF](#)

**Risoluzione del Parlamento Europeo del 25.11.2020 "Verso un mercato unico più sostenibile per le imprese e i consumatori":** [2021/1\(2\)GC](#)

**Risoluzione del Parlamento europeo del 21.01.2021 sul diritto dei lavoratori alla disconnessione:** [2021/1\(6\)LC](#)

**Riutilizzo di dati nel settore pubblico:** [2021/4\(4\)RA](#); [2022/1\(2\)RA](#); [2022/2\(1\)RA](#)

Rivoluzione digitale: [2021/1\(1\)DPDM](#)

Robo-advisory

Rome Call for AI Ethics: [2020/1\(7\)LC](#); [2020/4\(8\)SO](#)

## **S**

SaMD (Software as a Medical Device): [2021/4\(11\)SS](#)

Same activity, same risk, same regulation (principio): [2021/4\(10\)AF](#)

Sandbox: [2020/4\(5\)CR](#)

Sanità digitale: [2020/4\(5\)CR](#); [2022/3\(9\)CR](#); [2021/4\(11\)SS](#)

SARI (v. Sistema di riconoscimento facciale SARI Real Time)

Scopi di ricerca scientifica (diritto d'autore): [2022/1\(1\)EB](#)

Scorrimento pagina web: [2020/2\(5\)EMI](#)

Scroll (v. Scorrimento pagina web)

Securities Act of 1933 (USA) : [2022/4\(17\)EMI](#)

Securities Exchange Commission (SEC): [2022/2\(11\)AF](#); [2022/4\(17\)EMI](#)

Segreto commerciale: [2021/4\(4\)RA](#)

Servizi correlati (a prodotti generatori di dati): [2022/3\(3\)RA](#)

Servizi di intermediazione di dati: [2021/4\(4\)RA](#); [2022/2\(1\)RA](#)

Servizi sanitari digitali: [2022/3\(9\)CR](#)

Servizi della società dell'informazione: [2020/3\(2\)FB](#)

Sezioni specializzate in materia di impresa (art. 1 D.Lgs. 16/2003): [2022/4\(4\)SO](#)

Shaping Europe's Digital Future (v. Comunicazione della Commissione europea  
Plasmare il futuro digitale dell'Europa)

Shapiro Josh (Attorney General State of Pennsylvania): [2022/4\(18\)RMo](#)

Sistema Pubblico d'identità Digitale (SPiD): [2020/1\(8\)EWDM](#)

Sistemi di IA: [2021/2\(1\)SO](#)

Sistemi di IA ad alto rischio: [2021/2\(1\)SO](#); [2022/2\(8\)ES](#); [2022/3\(1\)TDMCDV](#)

Sistemi di IA di categorizzazione biometrica: [2021/2\(1\)SO](#)

Sistemi di IA di identificazione biometrica: [2021/2\(1\)SO](#); [2021/4\(3\)CR](#); [2022/1\(8\)GDI](#)

Sistemi di raccomandazione (v. Recommender systems)

Sistemi di IA di riconoscimento delle emozioni: [2021/2\(1\)SO](#)

Sistema di riconoscimento facciale SARI Real Time: [2021/2\(3\)CR](#)

**Sistemi di IA di social scoring discriminatorio:** [2021/2\(1\)SO](#)

**Sistemi di IA distorsivi del comportamento umano e che cagionano un danno fisico o psicologico alle persone fisiche:** [2021/2\(1\)SO](#)

**Sistemi di videosorveglianza con riconoscimento facciale:** [2021/2\(1\)SO](#); [2021/4\(3\)CR](#)

**Smart Contracts:** [2020/1\(3\)EMI](#); [2021/4\(12\)BC](#); [2022/3\(6\)ES](#)

**Snippets (diritto d'autore):** [2020/4\(7\)LC](#); [2022/1\(1\)EB](#)

**Social media** (v. Social networks)

**Social networks:** [2021/1\(1\)DPDM](#); [2021/2\(5\)FP](#); [2022/1\(8\)GDI](#)

**Software:** [2021/2\(10\)EMI](#); [2021/4\(5\)EMI](#)

**Software as a Medical Device (SaMD):** [2021/4\(11\)SS](#)

**Solidarietà:** [2022/4\(5\)RA](#)

**Sorveglianza dei lavoratori:** [2022/4\(12\)VR](#)

**Sostenibilità:** [2021/1\(2\)GC](#); [2022/1\(5\)ST](#); [2022/2\(3\)AF](#); [2022/3\(5\)EMI](#); [2022/4\(5\)RA](#)

**South Africa's Companies and Intellectual Property Commission:** [2021/4\(6\)FG](#)

**Sovranità monetaria:** [2022/2\(3\)AF](#)

**Spagna:** [2021/3\(1\)DI](#)

**Spam:** [2022/3\(8\)CR](#)

**Sperimentazione fintech:** [2021/4\(9\)ES](#)

**SPiD** (v. Sistema Pubblico d'identità Digitale)

**Sportello unico:** [2022/2\(1\)RA](#)

**Supreme Court of the United States** (v. Corte Suprema degli Stati Uniti d'America)

**Stabilità monetaria e finanziaria internazionale:** [2021/4\(10\)AF](#)

**Stablecoin:** [2020/2\(8\)EP](#); [2022/2\(3\)AF](#); [2022/2\(11\)AF](#)

**Stati Uniti d'America:** [2022/1\(9\)CR](#); [2022/1\(10\)CR](#); [2022/2\(11\)AF](#); [2022/3\(10\)LC](#); [2022/4\(7\)ST](#); [2022/4\(18\)RMo](#); [2022/4\(17\)EMI](#)

**Statuto dei lavoratori (l. 300/1970):** [2022/4\(12\)VR](#)

**Strategia europea in materia di dati:** [2021/4\(4\)RA](#)

**Strumenti finanziari:** [2022/4\(13\)ES](#)

**Subfornitura:** [2022/4\(4\)SO](#)

**Suprema Corte del Popolo della Repubblica Popolare Cinese:** [2021/3\(4\)CM](#)

# T

## **TAR Campania**

- Sede di Napoli, Sez. III, sentenza n. 7003 del 14.11.2022 sull'uso di sistemi algoritmici nei procedimenti amministrativi: [2022/4\(15\)FDA](#)

## **TAR Lazio**

- Sede di Roma, Sez. I, sentenze n. 260 e 261 del 18.12.2019 – 10.1.2020 sul claim “Facebook è gratis e sempre lo sarà”: [2020/1\(4\)MG](#)
- Sede di Roma, Sez. III-bis, sentenza n. 7589 del 24.6.2021 su algoritmi e attività amministrativa (a proposito di procedure di mobilità nella Pubblica Amministrazione): [2021/4\(7\)FDA](#)
- Sede di Roma, Sez. I, sentenza n. 15317 del 18.11.2022 di annullamento del provvedimento n. 88529 del 9.11.2021 dell'AGCM (contestazione di pratiche commerciali scorrette a carico di Apple): [2022/4\(19\)AM-GD](#)
- Sede di Roma, Sez. I, sentenza n. 15326 del 18.11.2022 sul provvedimento n. 29890 del 16.11.2021 dell'AGCM (contestazione di pratiche commerciali scorrette a carico di Google): [2022/4\(19\)AM-GD](#)

**Targeting online:** [2021/1\(5\)RMo](#)

**Tecnologie a registro distribuito** (v. DLT)

**TDM:** [2022/1\(1\)EB](#); [2022/2\(5\)SO](#)

**Telemedicina:** [2020/4\(5\)CR](#); [2021/4\(11\)SS](#)

**Testate editoriali online:** [2022/1\(1\)EB](#); [2022/4\(11\)SO](#)

**Testo Unico della Finanza (D. Lgs. 58/1998):** [2022/4\(13\)ES](#)

**Texas:** [2022/4\(7\)ST](#)

**Text and Data Mining** (v. TDM)

**Titolare dei dati:** [2022/3\(3\)RA](#)

**Token:** [2021/2\(6\)EP](#); [2022/4\(17\)EMI](#)

**Token collegati ad attività:** [2021/2\(6\)EP](#); [2022/2\(3\)AF](#)

**Token collegati ad attività basati su valuta non europea:** [2022/2\(3\)AF](#)

**Token di moneta elettronica:** [2021/2\(6\)EP](#)

**Top System (caso):** [2021/4\(5\)EMI](#)

**Trade secret:** [2021/4\(4\)RA](#)

**Transazioni finanziarie cross-border:** [2021/4\(10\)AF](#)

**Trasferimento dati personali all'estero:** [2020/3\(1\)CR](#); [2022/1\(9\)CR](#); [2022/1\(10\)CR](#)

**Trasparenza dell'algoritmo:** [2021/3\(2\)SO-CS](#)

#### **Tribunale di Milano**

- Sentenza n.12623/2016 del 5.1.2017 in materia di diritto all'oblio: [2022/1\(12\)FG](#)
- Sez. I Civile, ordinanza del 9.2.2022 in materia di c.d. eredità o patrimonio digitale (recupero dei dati personali da account del defunto, procedura denominata "trasferimento" volta a consentire ai ricorrenti l'acquisizione delle credenziali d'accesso all'ID Apple): [2021/1\(9\)CM](#)
- Sez. Lavoro, sentenza n. 1018/2022 del 20.4.2022 su algoritmo e qualificazione del rapporto di lavoro subordinato (piattaforma Deliveroo): [2022/2\(12\)VP](#)

#### **Tribunale di Roma**

- Sez. XVII Imprese civ. ordinanza ex art. 700 c.p.c. dell'11.12.2019 (ordine a Facebook di riattivazione della pagina di CasaPound Italia e del profilo personale del suo amministratore): [2020/3\(3\)LC](#)
- Sez. XVII Imprese civ. ordinanza del 29.4.2020 (su reclamo ex art. 669 terdecies c.p.c.) di conferma del provvedimento cautelare dell'11.12.2019 ottenuto da Casapound nei confronti di Facebook: [2020/3\(3\)LC](#)
- Sez. XVII Imprese civ. ordinanza del 20.7.2022 in materia di NFT (caso Juventus): [2022/4\(16\)FG](#)

**TUF** (v. Testo Unico della Finanza)

**Tutela dei consumatori** (v. Diritto del consumo)

**Tutela degli investitori in cripto-attività** (v. Protezione degli investitori in cripto-attività)

**Tutela dei minori** (v. Protezione dei minori)

## **U**

**Ufficio dell'Unione Europea per la proprietà intellettuale** (v. EUIPO)

**UK** (v. Regno Unito)

**UK Patents Act 1977:** [2021/4\(6\)FG](#)

**Ulteriore trattamento dei dati personali:** [2022/4\(8\)CR](#); [2022/4\(9\)CAT](#)

**Unfair commercial practices directive** (v. Direttiva sulle Pratiche Commerciali Scorrette 2005/29/CE)

**Unfair Trade Practices and Consumer Protection Law (Stato della Pennsylvania, USA):** [2022/4\(18\)RMo](#)

**United States Court of Appeals Fifth Circuit:** [2022/4\(7\)ST](#)

**Università Luigi Bocconi di Milano:** [2021/4\(8\)VR](#)

**Università Sapienza di Roma:** [2020/4\(8\)SO](#)

**UCPD Unfair commercial practices directive** (v. Direttiva 2005/29/CE sulle pratiche commerciali scorrette)

**USA** (v. Stati Uniti d'America)

**User Generated Content (UGC) (diritto d'autore):** [2022/1\(1\)EB](#)

**Utente inattivo:** [2022/4\(18\)RMo](#)

**Utility token:** [2022/4\(17\)EMI](#)

**Utilizzo di materiale protetto in ambiente digitale nei settori dell'istruzione, della ricerca e della conservazione del patrimonio culturale (diritto d'autore):** [2022/1\(1\)EB](#)

**Utilizzo online delle pubblicazioni giornalistiche:** [2022/1\(1\)EB](#)

## V

**Valuta virtuale:** [2022/1\(7\)ES](#); [2022/4\(13\)ES](#)

**Verbalizzazione assembleare a distanza:** [2020/1\(2\)MP](#)

**Verifica umana nella rimozione e disabilitazione dei contenuti online (diritto d'autore):** [2022/1\(1\)EB](#)

**Videosorveglianza:** [2022/4\(12\)VR](#)

**Virtual assistants** (v. Assistenti virtuali)

**Volgarizzazione del marchio:** [2022/4\(16\)FG](#)

## W

**Wallet di moneta virtuale:** [2022/4\(13\)ES](#)

**Web&App Activity (Google):** [2022/4\(18\)RMo](#)

**Web scraping:** [2022/1\(8\)GDI](#)

**Whistleblowing:** [2022/4\(2\)VR](#)

**Y**

**Yahoo:** [2022/1\(12\)FG](#)

**Youtube:** [2022/4\(19\)AM-GD](#)

**X**

**Z**

**1, 2, 3 ...**

**2018 Code of Practice on Disinformation:** [2022/4\(6\)DI](#)

**2018 Codice di buone pratiche sulla disinformazione:** [2022/4\(6\)DI](#)

**2022 Codice di buone pratiche sulla disinformazione rafforzato:** [2022/4\(6\)DI](#)

**2022 Strengthened Code of Practice on Disinformation:** [2022/4\(6\)DI](#)

**2030 Digital Compass:** [2022/4\(5\)RA](#)





