mediaLAWS

Rivista di diritto dei media
2/2023 ottobre

ANNO 2023 - CODICE ISSN 2532-9146
Impaginazione a cura di Chiara Pavesi

MediaLaws - Rivista di diritto dei media è una rivista quadrimestrale telematica, ad accesso libero, che si propone di pubblicare saggi, note e commenti attinenti al diritto dell'informazione italiano, comparato ed europeo.

La rivista nasce per iniziativa di Oreste Pollicino, Giulio Enea Vigevani, Carlo Melzi d'Eril e Marco Bassini e raccoglie le riflessioni di studiosi, italiani e stranieri, di diritto dei media.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Comittee on Publication Ethics).

La qualità e il rigore scientifici dei saggi della Rivista sono garantiti da una procedura di *double-blind peer review* affidata a un comitato di esperti per la valutazione individuato secondo criteri di competenza e rotazione e aggiornato ogni anno.

MediaLaws - Rivista di diritto dei media
Regolamento per la pubblicazione dei contributi

1. "MediaLaws – Rivista di diritto dei media" è una rivista telematica e ad accesso aperto che pubblica con cadenza quadrimestrale contributi attinenti al diritto dell'informazione.

2. Gli organi della rivista sono il Comitato di direzione, il Comitato scientifico e il Comitato degli esperti per la valutazione. L'elenco dei componenti del Comitato di direzione e del Comitato scientifico della rivista è pubblicato sul sito della stessa (rivista.medialaws.eu). Il Comitato degli esperti per la valutazione è sottoposto ad aggiornamento una volta l'anno.

3. La rivista si compone delle seguenti sezioni: "Saggi", "Note a sentenza" (suddivisa in "Sezione Europa", "Sezione Italia" e "Sezione comparata"), "Cronache e commenti" e "Recensioni e riletture". I singoli numeri potranno altresì ospitare, in via d'eccezione, contributi afferenti a sezioni diverse.

4. La sezione "Saggi" ospita contributi che trattano in maniera estesa e approfondita un tema di ricerca, con taglio critico e supporto bibliografico.

5. La sezione "Note a sentenza" ospita commenti alle novità giurisprudenziali provenienti dalle corti italiane, europee e straniere.

6. La sezione "Cronache e commenti" ospita commenti a questioni e novità giuridiche di attualità nella dimensione nazionale, europea e comparata.

7. La sezione "Recensioni e riletture" ospita commenti di opere rispettivamente di recente o più risalente pubblicazione.

8. La richiesta di pubblicazione di un contributo è inviata all'indirizzo di posta elettronica submissions@medialaws.eu, corredata dei dati, della qualifica e dei recapiti dell'autore, nonché della dichiarazione che il contributo sia esclusiva opera dell'autore e, nel caso in cui lo scritto sia già destinato a pubblicazione, l'indicazione della sede editoriale.

9. La direzione effettua un esame preliminare del contributo, verificando l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

10. In caso di esito positivo, la direzione procede ad assegnare il contributo alla sezione opportuna.

11. I saggi sono inviati alla valutazione, secondo il metodo del doppio cieco, di revisori scelti dall'elenco degli esperti per la valutazione della rivista secondo il criterio della competenza, della conoscenza linguistica e della rotazione. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore. La direzione garantisce l'anonimato della valutazione.

12. La direzione comunica all'autore l'esito della valutazione.
Se entrambe sono positive, il contributo è pubblicato.
Se sono positive ma suggeriscono modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. La direzione si riserva la facoltà di sottoporre il contributo così come modificato a nuova valutazione, anche interna agli organi della rivista. Se solo una valutazione è positiva, con o senza modifiche, la direzione si riserva la facoltà di trasmettere il contributo a un terzo valutatore. Se entrambe le valutazioni sono negative, il contributo non viene pubblicato.

13. Per pubblicare il contributo, l'Autore deve inviare una versione definitiva corretta secondo le regole editoriali della rivista pubblicate sul sito della stessa, un abstract in lingua italiana e inglese e un elenco di cinque parole chiave. Il mancato rispetto dei criteri editoriali costituisce motivo di rigetto della proposta.

14. Le valutazioni vengono archiviate dalla direzione della rivista per almeno tre anni.

15. A discrezione della direzione, i saggi di autori di particolare autorevolezza o richiesti dalla direzione possono essere pubblicati senza essere sottoposti alla procedura di referaggio a doppio cieco ovvero essere sottoposti a mero referaggio anonimo, previa segnalazione in nota.

Indice
Index

Editoriale

Sezione monografica
"Il *Digital Services Act* e il contrasto alla disinformazione: responsabilità dei *provider*, obblighi di *compliance* e modelli di *enforcement*"

Saggi

Note a sentenza

Cronache

Indice
Index

Editorial

Focus - The Digital Services "Act Regulation and the fight to disinformation: Internet service provider liability, compliance obligations and enforcement measures"

Essays

Case notes

Comments

Sono stati sottoposti a referaggio anonimo a doppio cieco i contributi di Emanuele Birritteri, Cristiana Carletti, Alessandro Cupri, Luca D'Agostino, Guido d'Ippolito, Giulia Formici, Vincenzo Iaia, Simone Poletti, Rossella Sabia, Laura Tadiotto, Andrea Tigrino, Domitilla Vanni, Chiara Vescovi, Pietro Villaschi, Silvia Vimercati, Silvio Roberto Vinceti

Editoriale

Il copyright al tempo dell'IA generativa

Francesco Posteraro

L'intelligenza artificiale può recare grandissimi benefici in termini di efficienza a numerosi comparti, dalla sanità alla tutela dell'ambiente, dai trasporti all'agricoltura, dalla sicurezza alla gestione delle infrastrutture e via dicendo. Nel contempo, come e forse più di quanto è accaduto per altre conquiste della tecnologia nell'era digitale, anche l'intelligenza artificiale può comportare gravi rischi per i diritti delle persone, tra i quali la *privacy* e la proprietà intellettuale, e per il sistema dell'informazione. Da qui la necessità che le istituzioni pubbliche intervengano per prevenire e mitigare i suddetti rischi. Purtroppo, di fronte a una tecnologia che evolve in maniera sempre più rapida, il compito del diritto assomiglia sovente alla fatica di Sisifo: fatica tanto più ardua se la si intraprende con ritardo, come si è verificato a proposito della rete internet, a lungo non sottoposta ad alcuna regolamentazione allo scopo di favorirne lo sviluppo.

L'IA generativa – ossia quella capace di produrre opere simili alle creazioni dall'ingegno umano – dà luogo a problemi che si riflettono sulla tutela del diritto d'autore e dei diritti connessi da un duplice punto di vista. Da un lato, si pone la questione della tutela dei diritti autoriali afferenti ai contenuti utilizzati per addestrare gli algoritmi. D'altro lato, ci si chiede se le opere prodotte dall'IA generativa possano a loro volta essere protette da diritto d'autore.

La possibilità di riconoscere la tutela del *copyright* a opere generate da sistemi di IA è destinata verosimilmente a trovare risposta, più e prima che nei testi legislativi, nelle aule dei tribunali. Alla luce di alcune recenti vicende processuali è già possibile tracciare una linea interpretativa. Mi riferisco in primo luogo alla decisione con la quale un tribunale federale di Washington ha respinto una domanda giudiziale volta a ottenere la protezione del *copyright* per un disegno generato da un sistema di IA denominato *Creativity Machine*, statuendo che solo alle opere create da autori umani possono riconoscersi i diritti d'autore. Il Copyright Office aveva motivato il diniego da cui ha tratto origine il giudizio con l'argomentazione che l'immagine generata da *Creativity Machine* non include alcun elemento di paternità umana. Dunque, nessuna tutela se l'opera è ascrivibile esclusivamente all'IA; se, invece, vi è un contributo dell'essere umano, allora la tutela può essere riconosciuta, ma all'uomo, non alla macchina.

Alle stesse conclusioni conduce un'ordinanza della I sezione civile della Corte di cassazione, la n. 1107 del 16 gennaio 2023, concernente l'utilizzazione da parte della RAI, quale scenografia per il Festival di Sanremo 2016, di un'opera grafica generata attraverso un *software*. Nel respingere il motivo di ricorso della RAI fondato su tale profilo – inammissibile perché non prospettato nel giudizio di merito – la Corte ha sostenuto, *incidenter tantum*, che l'uso di un *software* per generare un'immagine «è pur sempre compatibile con l'elaborazione di un'opera dell'ingegno con un tasso di creatività che andrebbe […] scrutinato». Per cui si rende necessario, argomenta la Corte,

«un accertamento di fatto per verificare se e in qual misura l'utilizzo dello strumento» abbia «assorbito l'elaborazione creativa dell'artista». Anche per la Corte di cassazione, dunque, la tutela del *copyright* spetta esclusivamente all'essere umano, e a condizione che la tecnologia digitale sia utilizzata – come si legge nell'ordinanza – soltanto come parte del processo creativo.

Così individuato il criterio al quale attenersi, la sua applicazione concreta rimane nondimeno tutt'altro che agevole, dovendosi stabilire, nei singoli casi, se l'apporto umano abbia o meno contribuito alla creazione dell'opera in misura sufficiente a determinare il riconoscimento della tutela. Di certo, non può bastare a questo fine l'aver progettato e messo in funzione l'algoritmo: la questione, altrimenti, non si porrebbe affatto, in quanto ci sarebbe comunque, in tutti i casi, un essere umano al quale far risalire la paternità dell'opera. Si consideri, al riguardo, che il 5 settembre scorso il Copyright Office ha negato la protezione a un'immagine creata da una IA denominata Midjourney nonostante essa fosse il risultato dell'inserimento nel sistema di un numero elevatissimo di *prompt*.

Problemi più complessi e soprattutto più delicati si pongono in ordine alla tutela dei diritti d'autore e dei diritti connessi concernenti i contenuti impiegati per addestrare gli algoritmi. Negli ultimi tempi il tema si è imposto all'attenzione di numerose istituzioni pubbliche, non soltanto europee. Pochi mesi or sono il Copyright Office USA ha dato avvio a un'iniziativa volta a esaminare i problemi creati dall'IA alla disciplina del *copyright*. La World Intellectual Property Organisation si è prefissa l'obiettivo di contribuire ad affrontare le sfide poste al diritto d'autore dall'IA generativa. Ancora negli USA, su richiesta dell'Amministrazione e in vista dell'emanazione di un *Executive Order* da parte del Presidente Biden, le aziende leader del settore dell'IA hanno sottoscritto nel luglio scorso una serie di impegni, nessuno dei quali però contempla la tutela del *copyright*.

Nel contempo molti titolari hanno adottato iniziative intese a tutelare i loro diritti. Negli USA scrittori, sceneggiatori e autori teatrali hanno intentato *class action* contro Open AI e in seguito contro Google. Nel Regno Unito Getty Images ha convenuto in giudizio la piattaforma Stability AI per l'utilizzo indebito di fotografie contenute nel suo database. Il New York Times e successivamente altri media – tra cui il Washington Post, la CNN, la Reuters, Espn, Bloomberg, Disney, nonché Radio France e TF1 – hanno vietato l'accesso ai propri siti al *crawler* di Open AI, ossia al *software* che copia i dati sul web e li analizza. Lo stesso New York Times – non avendo finora prodotto risultati il negoziato con Open AI volto a ottenere una remunerazione per l'accesso alla sua banca dati – sembra inoltre intenzionato ad agire in giudizio per i materiali che il sistema di IA ha utilizzato in passato.

Nel settore musicale appare invece avviata verso un accordo la trattativa tra Universal Music e Google volta alla realizzazione di una piattaforma che permetterebbe agli utenti di creare musica basandosi su brani già presenti sul mercato e ai titolari dei diritti di ottenere un ricavo per l'addestramento dell'algoritmo.

Se negli USA e nel Regno Unito la soluzione del problema sarà con ogni probabilità influenzata dagli esiti dei procedimenti giudiziari, nell'UE è stato avviato fin dall'aprile 2021 l'iter di un regolamento, l'AI Act, volto ad assicurare che lo sviluppo della nuova tecnologia non rechi pregiudizio ai diritti e ai valori protetti dall'ordinamento europeo.

Quando è stata presentata la proposta di regolamento l'IA generativa non aveva ancora fatto la sua comparsa. Per disciplinarne l'uso, il PE ha approvato nel giugno scorso un emendamento – destinato probabilmente a essere accolto nel testo definitivo dell'AI Act – che reca l'obbligo per gli sviluppatori dei sistemi di GenAI di rendere noti i dati protetti da diritto d'autore utilizzati per addestrare gli algoritmi. Imponendo ai fornitori di sistemi di IA generativa soltanto un obbligo di trasparenza, l'emendamento non fornisce dunque alcuna indicazione in ordine alla liceità o meno dell'uso di contenuti protetti da *copyright*, ma si limita a fare salva la vigente normativa europea in materia di diritto d'autore. Alla quale occorre pertanto riferirsi per individuare le disposizioni applicabili nella fattispecie.

Deve innanzi tutto escludersi che nei confronti dell'utilizzazione dei contenuti da parte di un sistema di IA generativa i diritti d'autore e i diritti connessi possano trovare protezione nell'art. 17 della Direttiva *Copyright*. Tale utilizzazione non può infatti configurarsi in alcun modo come un atto di comunicazione al pubblico, lecito, ai sensi del citato art. 17, solo a condizione di essere stato previamente autorizzato dai titolari dei diritti.

La norma cui fare riferimento è invece quella dell'art. 4 della stessa direttiva, che prevede l'eccezione di *text and data mining*. Prevede, cioè, che sia consentita l'estrazione di testo e di dati da opere o da altri materiali cui si abbia legalmente accesso (compresi dunque i contenuti disponibili online), a meno che il loro utilizzo non sia stato espressamente riservato dai soggetti cui spettano i diritti esclusivi di riproduzione. I titolari dei diritti possono quindi, esercitando un *opt-out*, sottrarre le proprie opere all'operatività dell'eccezione ed evitarne in tal modo l'uso ai fini dell'addestramento dei sistemi di IA. In questo quadro, l'adempimento dell'obbligo di trasparenza di cui all'emendamento del PE può servire a verificare se siano stati utilizzati contenuti per i quali i titolari abbiano esercitato la riserva.

Non occorre sottolineare che un meccanismo di *opt-in* sarebbe stato assai più efficace dell'*opt-out* ai fini della tutela del *copyright*. E se si deve supporre che all'epoca i legislatori europei nulla sapessero del futuro avvento dell'IA generativa, l'AI Act avrebbe fornito l'occasione, a quanto pare purtroppo non colta, per cambiare rotta in direzione di una più energica difesa dei diritti autoriali.

La direttiva precisa che i titolari dei diritti devono esercitare la riserva «in modo appropriato, ad esempio attraverso strumenti che consentano una lettura automatizzata in caso di contenuti resi pubblicamente disponibili sul web». L'art. 70-*quater* della legge sul diritto d'autore, con il quale è stato recepito nell'ordinamento italiano l'art. 4 della direttiva, non reca invece alcuna prescrizione in proposito. Con riferimento ai contenuti disponibili online l'impiego di strumenti tali da consentire una lettura automatizzata sembra tuttavia indispensabile per rendere possibile il riconoscimento della riserva da parte dei *crawler*.

Nei singoli Paesi membri dell'UE l'eccezione di *text and data mining* opera ovviamente a decorrere dal recepimento della direttiva nei rispettivi ordinamenti nazionali. Ciò significa che l'utilizzo di contenuti protetti da *copyright* avvenuto prima del suddetto recepimento deve considerarsi illecito; e può invece ritenersi lecito, a partire dal recepimento, a condizione che – e fino a quando – i titolari dei diritti non abbiano esercitato l'*opt-out*.

Relativamente all'accertamento delle eventuali violazioni dei diritti commesse prima dell'entrata in vigore dell'eccezione di *text and data mining* si pone però un problema di prova pressoché insolubile. Anche nel caso di *web scraping* eseguiti lecitamente sussistono peraltro difficoltà probatorie con riferimento al rispetto dell'obbligo – sancito dall'art. 4, par. 2, della Direttiva *Copyright* – di conservare le riproduzioni solo per il tempo necessario ai fini dell'estrazione di testo e di dati.

Quanto alle eventuali violazioni commesse dopo l'esercizio dell'*opt-out*, spetta alla tecnologia fare in modo di impedirle o almeno di individuarle. Nei confronti delle piattaforme e dei motori di ricerca designati come molto grandi a norma del DSA si potrebbe anche utilizzare a questo scopo la previsione dell'art. 37 di quel regolamento, che prevede la possibilità di sottoporre tali operatori a un *audit* esterno e indipendente.

Un'ultima notazione prima di concludere: assicurare la tutela dei diritti d'autore e dei diritti connessi può non equivalere, di fronte all'IA generativa, a tutelare anche i titolari. Non sembri un gioco di parole. Se pure dovesse continuare a svilupparsi rispettando il *copyright*, e dunque acquisendo i contenuti protetti solo in accordo con i titolari e dietro compenso, l'IA potrebbe comunque fare concorrenza all'industria culturale e quindi rischiare nel tempo di impoverirla. E il gioco non sarebbe in questo caso a somma zero, perché trovando nei settori creativi minori risorse cui attingere i sistemi di IA finirebbero nel lungo termine per produrre a loro volta contenuti di più modesta qualità. L'auspicio è che il diritto e la tecnologia sappiano scongiurare l'avverarsi di questo scenario distopico.

Sezione monografica

Il *Digital Services Act* e il contrasto alla disinformazione: responsabilità dei *provider*, obblighi di *compliance* e modelli di *enforcement*

Contenuti, scopi e traiettoria della ricerca: le nuove frontiere della *compliance* nel mercato digitale*

Antonio Gullo

La lotta alla disinformazione deve necessariamente incentrarsi sul coinvolgimento proattivo delle piattaforme e sulla *partnership* pubblico-privato. Questo approccio è dettato dall'uso (limitato) che deve essere fatto dello strumento penale in un settore per definizione sensibile, in cui si staglia sullo sfondo la necessità di non limitare la libertà di espressione. Il punto di partenza è che lo *ius terribile* non può essere utilizzato per sanzionare la mera diffusione di notizie false e proteggere di per sé la sola veridicità dell'informazione, a meno che tali condotte non arrechino pregiudizio ad altri beni giuridici meritevoli di tutela penale. Occorre, però, che il mandato in tal senso conferito alle piattaforme non assuma le caratteristiche di una 'delega in bianco'. Al contrario, è necessario che il potere di autonormazione e autoorganizzazione in funzione preventiva delle *corporation* sia esercitato entro i confini di una cornice pubblicistica di riferimento, in grado di delineare con sufficiente precisione le regole del gioco.

È questo il nocciolo duro dell'analisi svolta nel corso dei primi due cicli della sezione giuridica di questa ricerca[1]; si tratta adesso di proiettare lo sguardo verso l'attuale orizzonte normativo che, come noto, vive una stagione di cambiamento.

Il riferimento è naturalmente al regolamento (UE) 2022/2065 relativo al mercato unico dei servizi digitali (*Digital Services Act* – DSA) del 19 ottobre 2022, che ha cercato di

* Il presente report costituisce la sezione giuridica del terzo ciclo della ricerca dal titolo "Come individuare e contrastare operazioni coordinate di disinformazione in Italia. Casi di studio e indicazioni di policy per istituzioni pubbliche e private", condotta nell'A.A. 2022/2023 da ricercatori dell'Università Luiss Guido Carli, della Harvard Kennedy School e della School of Information dell'Università del Michigan. La ricerca è stata realizzata con un contributo dell'Unità di Analisi, Programmazione e Documentazione Storica del Ministero italiano degli Affari Esteri e della Cooperazione Internazionale (MAECI), ai sensi dell'art. 23-*bis* del d.p.r. n. 18 del 5 gennaio 1967. Le riflessioni contenute in questa ricerca riflettono esclusivamente la visione degli autori e non sono necessariamente rappresentative dell'opinione del MAECI e delle altre istituzioni coinvolte. Si ringraziano l'Unità di Analisi, Programmazione e Documentazione Storica del MAECI e gli altri Direttori della ricerca (Irene Pasquetto, Gianni Riotta e Costanza Sciubba Caniglia) per avere consentito la pubblicazione degli scritti in questa sede.

[1] V., per una sintesi, il contributo di apertura della sezione del fascicolo (n. 4/2021) della rivista *Diritto penale contemporaneo – Rivista trimestrale* in cui sono stati pubblicati gli esiti del primo ciclo della ricerca (cui si rinvia, unitamente ai tre lavori pubblicati in tale rapporto finale e richiamati nelle note successive, per tutti i riferimenti anche bibliografici): A. Gullo - G. Piccirilli, *Disinformazione e politiche pubbliche: una introduzione*, in *Diritto penale contemporaneo – Rivista trimestrale*, 4, 2021, 248 ss. Il report del secondo ciclo di studi è invece reperibile online in *esteri.it*.

rispondere proprio all'esigenza, sopra ricordata, e da più parti evocata, di regolamentare i modelli di *business* digitale nel tentativo di bilanciare il libero sviluppo di simili attività economiche nell'EU *single market* con la tutela dei rilevanti interessi individuali e collettivi (dal benessere psico-fisico della persona, alla tutela dell'integrità dei processi elettorali, fino a salute e sicurezza pubbliche) su cui tali nuove dinamiche sociali e di mercato sono in grado, come noto, di incidere significativamente.

L'obiettivo di fondo è duplice: da un lato, fornire al lettore e alle organizzazioni cui questo studio è rivolto una "guida ragionata" per muoversi all'interno delle molteplici novità normative introdotte dal Regolamento e per avere un quadro delle peculiari responsabilità di *enforcement* previste a loro carico; dall'altro lato, rimodulare – alla luce di tale importante riforma – le indicazioni di *policy* finali per istituzioni pubbliche e private formulate nel corso dei primi due anni del progetto di ricerca, al fine di aiutare i vari attori del sistema a identificare le migliori pratiche per assicurare un contrasto efficace alle azioni (coordinate e non) di disinformazione.

L'analisi sarà quindi divisa in tre capitoli volti a esaminare le altrettante macro-sezioni d'interesse in cui si articola il DSA, cercando altresì di evidenziarne punti di forza e limiti, anche tenuto conto degli esiti dei precedenti cicli dell'indagine.

La prima parte[2] si concentrerà sul regime di responsabilità dei *provider* e su alcuni specifici obblighi di *compliance* gravanti su tali operatori soprattutto per quanto attiene alla cooperazione con le autorità pubbliche. Si avrà qui modo di constatare tra l'altro come, a fronte della decisione di confermare quella che è ormai una impostazione consolidata della materia, e cioè l'assenza di obblighi generali di sorveglianza a carico dei fornitori, il DSA preveda alcune novità in punto sia di definizione di singoli profili della c.d. esenzione condizionata da responsabilità degli operatori, sia in termini, *inter alia*, di nuovi obblighi di attivazione (ad es. con riferimento alla doverosa notifica di sospetti reati che comportino una minaccia per la vita o la sicurezza di una o più persone, di cui il *provider* venga a conoscenza, ai sensi e per gli effetti dell'art. 18 del Regolamento).

Il secondo contributo[3], poi, sarà dedicato allo studio dell'impatto del DSA sulle attività di *private enforcement* dei soggetti regolati rispetto alla moderazione dei contenuti immessi in rete dagli utenti. A differenza di quanto accaduto per il modello di responsabilità del *provider*, da questo angolo visuale le innovazioni sono molte e di grande rilievo, avendo qui il legislatore europeo cercato di costruire quella cornice normativa pubblicistica, cui pocanzi si alludeva, entro la quale le piattaforme esercitano la loro potestà di regolare, tra l'altro, il dibattito pubblico e il confronto politico che si svolge nelle rispettive arene digitali.

Obiettivo, quest'ultimo, che viene perseguito scommettendo sui paradigmi, sulle prassi, sulle metodiche della *corporate compliance*, con la significativa decisione di diversificare le *due diligence obligation* degli operatori attraverso una peculiare struttura di adempimen-

[2] L. D'Agostino, *Disinformazione e obblighi di* compliance *degli operatori del mercato digitale alla luce del nuovo* Digital Services Act*,* in questa medesima sezione monografica, in *questa Rivista,* 2, 2023.

[3] E. Birritteri, *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di* compliance *e dei poteri di autonormazione degli operatori,* in questa medesima sezione monografica, in *questa Rivista,* 2, 2023.

ti a strati progressivi, in cui il regolatore eurounitario stabilisce man mano obblighi più stringenti al crescere dell'importanza strategica del soggetto regolato (che si aggiungono, e non si sostituiscono a quelli dei livelli precedenti): dalle previsioni minimali valide per tutti i prestatori di servizi intermediari fino all'anello finale delle misure concernenti esclusivamente le c.d. VLOPs (*Very Large Online Platforms*) e i c.d. VLOSEs (*Very Large Online Search Engines*).

Si va, a seconda dei casi, dagli obblighi in punto di definizione di termini e condizioni del servizio, di predisposizione di meccanismi di *notice and action* e di sistemi interni di gestione dei reclami, fino a quelli di valutazione e gestione dei rischi a carattere sistemico legati ai servizi digitali, sottoposizione ad *audit* indipendenti, istituzione di una specifica funzione aziendale di DSA *compliance*, e via discorrendo.

Questa scelta, per certi versi, è esemplificativa della natura 'liquida' della *compliance*, capace di imporsi sempre più come modello di regolazione vincente in diversi settori e a carattere trasversale (costituendo la cifra distintiva oramai di numerosi ambiti di disciplina, tra cui sicurezza sul lavoro, *privacy*, responsabilità da reato degli enti). Ciò, peraltro, secondo cadenze che vedono sempre più il settore di volta in volta toccato dall'innesto della logica della *compliance* preventiva conformarsi alle note distintive di questo particolare meccanismo di gestione del rischio, latamente inteso, piuttosto che il contrario. Insomma, è l'ambito in cui la *compliance* viene importata a essere plasmato da queste metodologie – fatte di processi e procedure, analisi e gestione del rischio, monitoraggi tramite un sistema strutturato di controlli e revisioni –, che invece percorrono 'indenni' gli ordinamenti e i contesti in cui vengono applicate, senza mutare il proprio DNA.

L'ultima sezione della ricerca[4], infine, è dedicata all'*enforcement* pubblico del Regolamento, sia per ciò che concerne i poteri assegnati agli Stati membri, sia avuto riguardo a quelli conferiti alla Commissione europea, che assume il ruolo di interlocutore privilegiato per i procedimenti sanzionatori riguardanti le piattaforme online e i motori di ricerca online di dimensioni molto grandi. Come si vedrà, anche da tale versante il 'vento del cambiamento' ha soffiato forte, dal momento che la riforma cerca di sperimentare paradigmi punitivi peculiari, ispirati talvolta anche al modello ingiunzionale e alla volontà di testare forme più o meno strutturate di 'soluzioni negoziali' in relazione all'inosservanza del DSA, in un certo senso non dissimili da prassi largamente in uso in alcuni ordinamenti sul terreno della *corporate criminal liability*.

Soltanto l'esperienza applicativa potrà dirci se quello imboccato dal legislatore europeo sarà un percorso in grado di dare i frutti sperati. Il compito che ci si proponeva, del resto, non era e non sarà semplice specie allorquando, dalla prospettiva della *law in the books*, le nuove regole unionali si confronteranno con le dinamiche applicative.

Senza dubbio, però, il DSA colma finalmente una lacuna che, unitamente alle prospettive che oggi si stanno aprendo avuto riguardo all'*Artificial Intelligence Act*, rende l'Unione europea – e il suo *acquis* normativo che in questi casi assume carattere quasi pioneristico – un punto di riferimento fondamentale nello scenario globale.

[4] V. R. Sabia, *L'*enforcement *pubblico del* Digital Services Act *tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni,* in questa medesima sezione monografica, in *questa Rivista,* 2, 2023.

Disinformazione e obblighi di *compliance* degli operatori del mercato digitale alla luce del nuovo *Digital Services Act**

Luca D'Agostino

Abstract

Il contributo esamina l'impatto del Digital Services Act sull'attività di private enforcement per la moderazione dei contenuti immessi in rete dagli utenti – con la correlata due diligence – svolta dagli operatori digitali. Vengono analizzati fondamento, contenuti e limiti degli obblighi di compliance e dei poteri di autonormazione attribuiti al riguardo ai vari attori del sistema, mettendone in evidenza punti di forza e criticità con particolare riferimento alle strategie di contrasto alla disinformazione in rete. La parte finale dello scritto delinea alcune indicazioni di policy rivolte ai soggetti che saranno chiamati a conformarsi alle previsioni del nuovo Regolamento europeo.

This article aims at analysing the impact of the Digital Services Act on private enforcement activities for the moderation of user content – with the related due diligence – carried out by digital operators. In particular, the contribution examines the basis, content and limits of compliance obligations and self-regulatory powers attributed to the various actors involved, highlighting strengths and weaknesses, with a focus on strategies for combating disinformation online. The final part of the paper outlines some policy recommendations for subjects that will be required to comply with the provisions of this new European regulation.

Sommario

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

(VLOPs) e dei *Very Large Online Search Engines* (*VLOSEs*): la scommessa del legislatore europeo sulla *compliance*. – 4.1. Obblighi di *risk assessment*. – 4.2. Le previsioni in punto di mitigazione dei rischi. – 4.3. Il *crisis response mechanism*. – 4.4. L'*Independent audit*. – 4.5. L'istituzione di una specifica funzione aziendale di *compliance* per monitorare la conformità dell'organizzazione agli obblighi del DSA. – 5. Riflessioni conclusive e indicazioni di *policy*.

Keywords

Digital Services Act – *Compliance* – Autonormazione – *Due diligence* – *Private enforcement*

1. L'impatto del DSA sulle attività di *private enforcement* per il contrasto alla disinformazione: inquadramento generale

Nel corso dei primi due cicli della sezione giuridica di questa ricerca abbiamo rilevato come l'implementazione di strategie di contrasto alla disinformazione in rete non possa che fare affidamento sul coinvolgimento proattivo delle piattaforme online e degli operatori del mercato digitale, nella consapevolezza, come abbiamo cercato di dimostrare, dell'impossibilità di utilizzare il diritto criminale per punire di per sé la diffusione di notizie false, fuori dai casi in cui ciò arrechi pregiudizio ad interessi diversi dalla mera veridicità dell'informazione e per cui si ritenga possibile e necessaria la tutela penale[1].

Abbiamo altresì messo in luce come i decisori pubblici e gli studiosi del diritto punitivo debbano oggi necessariamente occuparsi delle pratiche di *private enforcement* tipiche di tale settore, dato che le attività di moderazione dei contenuti immessi in rete dagli utenti, realizzate soprattutto dalle grandi *corporation* digitali, possono incidere in misura significativa sui diritti fondamentali degli utenti (su tutti, la libertà di espressione), nel contesto di grandi arene digitali che, pur gestite da organizzazioni private, rappresentano oggi uno spazio di dibattito pubblico di rilevante importanza[2]. Ciò, inevitabilmente, finisce per "consegnare" nelle mani di tali *Big Tech* un grande potere, avendo tali soggetti collettivi la possibilità di farsi arbitri di tali dinamiche di interazione sociale e di esercitare una potestà "sanzionatoria" – in termini di rimozione di contenuti, disabilitazione di *account* anche di rilevanti personaggi politici, etc. – che può innescare un pericoloso *chilling effect* avuto riguardo al libero confronto democratico[3].

Di qui la necessità di costruire una cornice di regolazione pubblica volta a fissare le regole del gioco in materia, nell'ambito della quale gli operatori possano svolgere tali

[1] Sia consentito, anche per una più ampia *literature review*, il rinvio a E. Birritteri, *Punire la disinformazione: il ruolo del diritto penale e delle misure di moderazione dei contenuti delle piattaforme tra pubblico e privato*, in *Diritto penale contemporaneo – Rivista Trimestrale*, 4, 2021, 304 ss.

[2] A. Gullo - G. Piccirilli, *Disinformazione e politiche pubbliche: una introduzione*, in *Diritto penale contemporaneo – Rivista Trimestrale*, 4, 2021, 248 ss.

[3] A. Gullo - G. Piccirilli, *ivi*, 249. In argomento v. anche A. Buratti, *Framing the Facebook Oversight Board: Rough Justice in the Wild Web?*, in questa *Rivista*, 2, 2022, 31 ss.

attività di autonormazione e "sanzionatorie" secondo regole fissate dal legislatore e sotto il controllo delle autorità pubbliche[4].

Il nuovo regolamento (UE) 2022/2065 relativo al mercato unico dei servizi digitali (*Digital Services Act*, d'ora in poi DSA) del 19 ottobre 2022[5] cerca di rispondere esattamente a tale esigenza, da un lato, prendendosi atto che gli «Stati membri stanno sempre più introducendo o stanno valutando di introdurre legislazioni nazionali sulle materia disciplinate dal presente Regolamento, imponendo in particolare obblighi di diligenza per i prestatori di servizi intermediari per quanto riguarda il modo in cui dovrebbero contrastare i contenuti illegali, la *disinformazione online* e altri rischi per la società»[6] e che alla luce «del carattere intrinsecamente transfrontaliero di internet […] tali legislazioni nazionali divergenti incidono negativamente sul mercato interno, che […] comporta uno spazio senza frontiere interne»[7]; dall'altro lato, riconoscendosi che, appunto, «un comportamento responsabile e diligente da parte dei prestatori di servizi intermediari è essenziale per un ambiente online sicuro, prevedibile e affidabile e per consentire ai cittadini dell'Unione e ad altre persone di esercitare i loro diritti fondamentali garantiti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), in particolare la libertà di espressione e di informazione, la libertà di impresa, il diritto alla non discriminazione e il conseguimento di un elevato livello di protezione dei consumatori»[8].

Obiettivo di questa sezione della presente ricerca è quello di esaminare l'impatto del DSA sull'attività di *private enforcement* per la moderazione dei contenuti immessi in rete dagli utenti – con la correlata *due diligence* – svolta dagli operatori digitali. Si tratta invero di pratiche che fino all'emanazione del regolamento europeo in questione venivano svolte di fatto in assenza di una disciplina legislativa di riferimento, nonostante si trattasse e si tratti della prima (e soprattutto sovente anche unica) barriera "sanzionatoria" di contrasto alla diffusione della disinformazione in rete[9].

In linea generale, il primo effetto tangibile di questo regolamento su tali pratiche è determinato dall'art. 3, lett. t), che fornisce direttamente una definizione di «moderazione dei contenuti» –inquadrando così chiaramente, sul versante legislativo, il fenomeno che costituisce il *focus* di questa sezione del report – come «le attività, automatizzate o meno, svolte dai prestatori di servizi intermediari con il fine, in particolare, di individuare, identificare e contrastare contenuti illegali e informazioni incompatibili con

---

4 Necessità che abbiamo ribadito anche all'esito del secondo ciclo della ricerca: v. il report del 2022, reperibile online in *esteri.it*.

5 Per un primo inquadramento generale v. anche B. Tassone, *Riflessioni introduttive*, in *Diritto di internet*, 1, 2023, 3 ss. Nella letteratura internazionale v., ampiamente, anche per ulteriori riferimenti circa le varie implicazioni del nuovo regolamento, A. Turillazzi - M. Taddeo - L. Floridi - F. Casolari, *The digital services act: an analysis of its ethical, legal and social implications*, in *Law, Innovation and Technology*, 15(1), 2023, 83 ss.

6 Cfr. il considerando 2 del regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), GU 2022 L 277/1 (corsivo nostro).

7 V. sempre il considerando 2 del regolamento (UE) 2022/2065.

8 Così il considerando 3 del regolamento (UE) 2022/2065.

9 Per una più ampia analisi, sia consentito rinviare ancora a E. Birritteri, *Punire la disinformazione*, cit., 304 ss.

le condizioni generali, forniti dai destinatari del servizio, comprese le misure adottate che incidono sulla disponibilità, sulla visibilità e sull'accessibilità di tali contenuti illegali o informazioni, quali la loro retrocessione, demonetizzazione o rimozione o la disabilitazione dell'accesso agli stessi, o che incidono sulla capacità dei destinatari del servizio di fornire tali informazioni, quali la cessazione o la sospensione dell'account di un destinatario del servizio»[10].

Il Capo III del regolamento, poi, disciplina in dettaglio tutta una serie di *due diligence obligations* relative, tra l'altro, proprio a tali attività di *private enforcement*, con un sistema di obblighi strutturato secondo vari "livelli" di intensità crescente in base al particolare destinatario degli stessi, dalla dimensione "base" delle previsioni applicabili a tutti i prestatori di servizi intermediari fino all'ultimo "gradino" concernente le più gravose regole applicabili alle piattaforme online e ai motori di ricerca di "dimensioni molto grandi". In particolare, il passaggio a ogni livello successivo comporta la sottoposizione dell'operatore all'obbligo di conformarsi ad alcune disposizioni ulteriori che si aggiungono (e *non* si sostituiscono) a quelle degli stadi precedenti[11].

Nei paragrafi successivi descriveremo, quindi, i principali contenuti di tali obblighi di diligenza, cercando di metterne in evidenza punti di forza e limiti anche alla luce degli esiti dell'indagine svolta durante i primi due cicli della presente ricerca, per poi delineare, in conclusione, alcune indicazioni di *policy*.

1.1. Obblighi in punto di definizione di termini e condizioni del servizio

Come noto, la sezione 1 del Capo III del DSA riguarda le disposizioni applicabili a tutti i prestatori di servizi intermediari.

La prima previsione che viene in considerazione in relazione all'oggetto di tale sezione della ricerca è senz'altro l'art. 14, che impone ai detti operatori di includere, con un linguaggio chiaro, semplice, comprensibile e adatto se del caso anche ai minori, nelle loro condizioni generali di erogazione del servizio, ogni informazione relativa a: a) tutte le politiche, le procedure e gli strumenti utilizzati nel moderare i contenuti immessi in rete dagli utenti, con informazioni specifiche sul «processo decisionale algoritmico e la verifica umana»[12]; c) le regole procedurali del loro sistema interno di gestione dei

[10] Lo stesso art. 3, poi, per quanto qui interessa fornisce sia, alla lett. h), la definizione di contenuto illegale come «qualsiasi informazione che, di per sé o in relazione a un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro conforme con il diritto dell'Unione, indipendentemente dalla natura o dall'oggetto specifico di tale diritto», sia, alla lett. u), quella di 'condizioni generali' come «tutte le clausole, comunque denominate e indipendentemente dalla loro forma, che disciplinano il rapporto contrattuale tra il prestatore dei servizi intermediari e il destinatario del servizio».

[11] Giustamente in dottrina si è subito parlato di approccio '*pyramid base*': v. M.L. Bixio, *Gli obblighi applicabili a tutti i prestatori di servizi intermediari, ai prestatori di servizi di* hosting *e ai fornitori di piattaforme* online *(Artt. 11-32 – Capo III, Sezioni, 1, 2, 3 e 4)*, in *Diritto di internet*, 1, 2023, 21.

[12] Con una disposizione che evoca chiaramente i contenuti di cui all'art. 22 del GDPR, e l'esigenza quindi di una specifica forma di trasparenza in relazione ai principi ivi sanciti, che stabiliscono il diritto dell'interessato a non essere sottoposto a decisioni basate su trattamenti integralmente automatizzati

reclami[13].

È significativo notare come il legislatore europeo imponga a tali soggetti regolati, in definitiva, un obbligo di trasparenza rispetto alla necessità di informare i loro utenti sulle politiche connesse alla moderazione dei contenuti immessi in rete e sul funzionamento dei relativi mezzi di reclamo. Nulla si dice, quindi, sulle specifiche caratteristiche di dettaglio che tali procedure di *private enforcement* debbano avere, sui "connotati" dei processi di moderazione e su quelli, conseguenti, di reclamo da parte dell'utente rispetto alla decisione della piattaforma di imporre una restrizione sull'informazione immessa in rete. In tal senso, in questa previsione il DSA non impone modelli particolari.

Gli operatori, di conseguenza, rimangono sostanzialmente liberi di regolare nel modo da loro ritenuto più opportuno tanto i meccanismi di moderazione dei contenuti degli utenti, quanto i correlati strumenti di reclamo, dovendo però, nel farlo, come si legge al paragrafo 4 dell'art. 14 con una indicazione tanto generale quanto importante, agire «in modo diligente, obiettivo e proporzionato» e «tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte, compresi i diritti fondamentali dei destinatari del servizio, quali la libertà di espressione, la libertà e il pluralismo dei media, e altri diritti e libertà fondamentali sanciti dalla Carta»[14].

La scelta di *policy* qui fatta propria dal decisore eurounitario ci pare presenti aspetti positivi e alcune criticità.

Da un lato, invero, introdurre specifiche procedure di dettaglio sul piano della moderazione dei contenuti e dei reclami, valide per qualsiasi prestatore di servizi intermediari a prescindere dallo specifico mercato di riferimento, dal tipo di attività, dalla dimensione, secondo un modello *one size fits all*, sarebbe stato molto rischioso e, forse, controproducente, con il rischio di imporre oneri eccessivamente gravosi e non necessari[15]; anche il richiamo esplicito alla libertà di espressione e al pluralismo dei media, poi, appare molto importante specie sul piano del contrasto alla disinformazione, sensibilizzando gli operatori sulla necessità di adottare un approccio molto prudente e attento al rispetto dei diritti fondamentali nel disciplinare e applicare tali *policy* che, come ricordavamo, possono avere un impatto molto significativo su simili *fundamental rights* e generare un

che producano effetti che incidano sulla sua sfera giuridica, imponendo che tale automazione sia in tal senso parte di una procedura valutativa più ampia che, tra l'altro, preveda necessariamente l'intervento umano.

[13] I parr. 5 e 6 dell'art. 14 dettano poi alcune specificazioni di dettaglio ulteriori per le piattaforme e i motori di ricerca molto grandi «I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi forniscono ai destinatari dei servizi una sintesi concisa delle condizioni generali, di facile accesso e leggibile meccanicamente, compresi le misure correttive e i mezzi di ricorso disponibili, in un linguaggio chiaro e privo di ambiguità. Le piattaforme online di dimensioni molto grandi e i motori di ricerca online di dimensioni molto grandi ai sensi dell'articolo 33 pubblicano le loro condizioni generali nelle lingue ufficiali di tutti gli Stati membri in cui offrono i loro servizi». In linea generale, poi, la disposizione obbliga i prestatori a informare i destinatari di ogni significativa variazione in merito alle condizioni generali del servizio.

[14] È significativo evidenziare come ai sensi del considerando 47 del DSA, nel «progettare, applicare e far rispettare [le] restrizioni […] i prestatori di servizi intermediari dovrebbero inoltre tenere debitamente conto delle pertinenti norme internazionali in materia di tutela dei diritti umani, quali i principi guida delle Nazioni Unite su imprese e diritti umani».

[15] Su questi temi si veda diffusamente anche P. Leerssen, *An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation*, in *Computer Law & Security Review*, 48, 2023, 6.

pericoloso e non auspicale *chilling effect*.
Dall'altro lato, però, pur senza legittimare inutili irrigidimenti burocratici, sarebbe stato a nostro avviso utile aggiungere qualche specificazione in più in merito ai "diritti di garanzia" minimali dell'utente sul piano delle misure che la piattaforma può disciplinare e adottare incidendo sui suoi diritti fondamentali (su tutti, dalla nostra prospettiva, la libertà di espressione). Nelle indicazioni di *policy* che avevamo formulato al termine dei precedenti due cicli della presente ricerca, ad esempio, avevamo menzionato sul punto, tra l'altro, come minimo «il principio di legalità delle violazioni e delle misure sanzionatorie/interdittive, con i relativi corollari della irretroattività, della tassatività/precisione delle previsioni punitive, e del divieto di analogia, nonché con una chiara definizione dei soggetti titolari della potestà di dettare tali regole; il principio di proporzionalità del trattamento sanzionatorio rispetto alla concreta gravità della violazione; il divieto di responsabilità oggettiva e l'affermazione del principio di colpevolezza, con la necessità di specificare l'elemento soggettivo (dolo o colpa) necessario per integrare la violazione»[16]. Come avremo modo di evidenziare a breve, su taluni di tali profili alcune disposizioni aggiuntive previste dal DSA e applicabili a certi operatori sembrano offrire soluzioni più soddisfacenti, ma tale prima previsione restituisce l'impressione di una non del tutto compiuta valorizzazione di profili di non secondaria importanza per una efficace protezione degli utenti. Del resto, sul versante specifico del contrasto alla disinformazione, è proprio su tali preliminari aspetti – *i.e.*, sulla determinazione dei principi di comportamento degli utenti e delle modalità d'uso del servizio, piuttosto che esclusivamente sul successivo *private enforcement* di tali regole – che i decisori pubblici sono chiamati a misurarsi con le più delicate ripercussioni dell'esercizio da parte delle *corporation* tecnologiche di tale potestà di autoregolare il dibattito pubblico e il confronto politico che si svolge sulle loro reti, con tutti i rischi di censura e di impatto negativo sui diritti fondamentali che ciò comporta[17].

1.2. Relazioni di trasparenza

La sezione 1 del Capo III del DSA prevede all'art. 15 un ulteriore obbligo di *due diligence* per tutti i prestatori di servizi intermediari[18], afferente al nostro ambito di interesse: si tratta del dovere di pubblicare, almeno una volta all'anno, «relazioni chiare e facilmente comprensibili sulle attività di moderazioni dei contenuti svolte durante il periodo di riferimento».
Tali relazioni devono comprendere una serie di informazioni su, tra l'altro: *a)* le attività di moderazione di contenuti avviate di propria iniziativa anche mediante l'uso di stru-

[16] Vedi testualmente l'indicazione di *policy* n. 20, nella versione del report della ricerca del 2022, reperibile online in *esteri.it*.

[17] A.P. Heldt, *EU Digital Services Act: The White Hope of Intermediary Regulation*, in T. Flew - F.R. Martin (a cura di), *Digital Platform Regulation. Global Perspectives on Internet Governance*, Cham, 2022, 79.

[18] Il par. 2 dell'art. 15 peraltro stabilisce che «Il paragrafo 1 del presente articolo non si applica ai prestatori di servizi intermediari che si qualificano come microimprese o piccole imprese come definite nella raccomandazione 2003/361/CE e che non sono piattaforme online di dimensioni molto grandi a norma dell'articolo 33 del presente regolamento».

menti automatizzati; per qualsiasi utilizzo di questi ultimi nelle attività di moderazione, peraltro, si devono fornire dettagli concernenti «la descrizione qualitativa, la descrizione delle finalità precise, gli indicatori di accuratezza e il possibile tasso di errore degli strumenti automatizzati utilizzati nel perseguimento di tali scopi e le eventuali garanzie applicate»; *b)* le misure implementate per fornire una specifica formazione e assistenza alle persone dell'organizzazione incaricate di svolgere tale attività di *private enforcement*; *c)* il numero e il tipo di "sanzioni" irrogate agli utenti avuto riguardo a ogni restrizione all'uso del servizio, con la necessità, tra l'altro, di classificare e differenziare tali informazioni in base alle diverse tipologie di contenuto illegale o alle specifiche regole interne della piattaforma violate, nonché con riferimento al metodo di rilevamento dell'inosservanza; *d)* il numero di reclami ricevuti[19]. Per le piattaforme online e i motori di ricerca "di dimensioni molto grandi", in linea con gli obblighi aggiuntivi per loro previsti[20], si prevedono altresì misure ancor più stringenti in merito ai contenuti e alle tempistiche di tale relazione[21].

---

[19] In base alle lett. a) e b) del par. 1 dell'art. 15, inoltre, occorre indicare «a) per i prestatori di servizi intermediari, il numero di ordini ricevuti dalle autorità degli Stati membri, compresi gli ordini emessi a norma degli articoli 9 e 10, classificati in base al tipo di contenuti illegali in questione, lo Stato membro che ha emesso l'ordine e il tempo medio necessario per informare l'autorità che ha emesso l'ordine o qualsiasi altra autorità specificata nell'ordine in merito al suo ricevimento e per dare seguito allo stesso; b) per i prestatori di servizi di memorizzazione di informazioni, il numero di segnalazioni presentate a norma dell'articolo 16, classificate in base al tipo di contenuto illegale presunto di cui trattasi, il numero di segnalazioni presentate da segnalatori attendibili, nonché eventuali azioni intraprese in applicazione delle segnalazioni, specificando se l'azione sia stata avviata in virtù di disposizioni normative oppure delle condizioni generali del prestatore, il numero di segnalazioni trattate utilizzando strumenti automatizzati e il tempo mediano necessario per intraprendere l'azione». Rispetto ai reclami, poi, la lett. d) stabilisce che è necessario anche menzionare «per i fornitori di piattaforme online, conformemente all'articolo 20, la base di tali reclami, le decisioni adottate in relazione a tali reclami, il tempo mediano necessario per adottare tali decisioni e il numero di casi in cui tali decisioni sono state revocate». Ai sensi dell'art. 24 del DSA, tra l'altro, i fornitori di piattaforme online devono includere alcune informazioni aggiuntive in tale relazione, tra cui il numero di controversie sottoposte all'esame degli organismi di risoluzione extragiudiziale e il numero di sospensioni imposte *ex* art. 23 DSA.

[20] Sui quali ci soffermeremo nel dettaglio *infra* (par. 4 e ss. del presente capitolo).

[21] L'art. 42 del DSA stabilisce, infatti, che questi operatori debbano pubblicare, in almeno una delle lingue ufficiali degli Stati membri, «le relazioni di cui all'articolo 15 al più tardi entro due mesi dalla data di applicazione di cui all'articolo 33, paragrafo 6, secondo comma, e successivamente almeno ogni sei mesi», specificando «oltre alle informazioni di cui all'articolo 15 e all'articolo 24, paragrafo 1: a) le risorse umane dedicate dal fornitore di piattaforme online di dimensioni molto grandi alla moderazione dei contenuti in relazione al servizio offerto nell'Unione, suddivise per ciascuna lingua ufficiale applicabile degli Stati membri anche per il rispetto degli obblighi di cui agli articoli 16 e 22, nonché per il rispetto degli obblighi di cui all'articolo 20; b) le qualifiche e le competenze linguistiche delle persone che svolgono le attività di cui alla lettera a), nonché la formazione e il sostegno forniti a tale personale; c) gli indicatori di accuratezza e le relative informazioni di cui all'articolo 15, paragrafo 1, lettera e), suddivisi per ciascuna lingua ufficiale degli Stati membri», nonché ulteriori informazioni concernenti il numero medio mensile dei destinatari del servizio, anche per ciascun Stato membro. Specifici obblighi di pubblicazione e comunicazione aggiuntivi si riferiscono poi, ai sensi dei parr. 4 e 5 dell'art. 42 del DSA, agli *independent audit* cui tali soggetti, come vedremo (cfr. infra par. 4.4.), devono sottoporsi, prevedendosi tra l'altro che qualora «un fornitore di piattaforme online di dimensioni molto grandi o di motori di ricerca online di dimensioni molto grandi ritenga che la pubblicazione di informazioni a norma del paragrafo 4 possa comportare la divulgazione di informazioni riservate di tale fornitore o dei destinatari del servizio, comportare notevoli vulnerabilità per la sicurezza del suo servizio, compromettere la sicurezza pubblica o danneggiare i destinatari, può rimuovere tali informazioni dalle relazioni disponibili al pubblico. In tal caso il fornitore trasmette le relazioni complete al coordinatore dei servizi digitali del luogo di stabilimento e alla Commissione, corredate di una spiegazione dei motivi

La commissione, inoltre, potrà adottare «atti di esecuzione per stabilire modelli relativi alla forma, al contenuto e ad altri dettagli delle relazioni a norma del paragrafo 1 del presente articolo, compresi periodi di comunicazione armonizzati», diffondendo quindi *best practice* operative e modelli standard di riferimento che potranno essere di concreto ausilio agli operatori per adeguarsi a tali obblighi di conformità.
Si tratta senz'altro di una previsione condivisibile ove l'obbligo di trasparenza imposto alle piattaforme muove dalla prospettiva *in the books* dell'art. 14 a quella, per così dire, *in action*, imponendosi una *disclosure* anche sul modo in cui le regole autonormate dalle piattaforme sull'attività di moderazione dei contenuti sono effettivamente applicate in concreto, nella quotidiana realtà operativa dell'organizzazione.
Ciò sembra poter consentire agli organi di *enforcement* di accedere a informazioni che hanno indubbiamente un peso specifico significativo per valutare se gli obblighi definiti dall'art. 14 del DSA siano effettivamente rispettati, pur rimanendo naturalmente ferme le perplessità sul margine di libero apprezzamento lasciato alle piattaforme nel definire, a monte, tali regole del gioco. Si tratta invero di un potere che non pare poter essere ridotto dal dovere, a valle, di pubblicare relazioni in merito alla concreta applicazione di misure costruite secondo una discrezionalità che rimane, come abbiamo rilevato, certamente ampia per larghi tratti.

2. Disposizioni aggiuntive applicabili ai prestatori di servizi di memorizzazione di informazioni, comprese le piattaforme online

Come osservato in apertura il DSA prevede una serie di doveri di diligenza a intensità crescente per gli operatori, che variano a seconda del tipo di soggetto regolato[22]; il passaggio a ogni nuovo livello comporta l'applicazione di obblighi aggiuntivi, che vanno a sommarsi a quelli dei "piani" precedenti. Il primo di tali "strati" di *obligation* aggiuntive è costituito dalle disposizioni della sezione II del capo III del DSA, concernente le regole applicabili ai prestatori di servizi di "memorizzazione di informazioni", comprese le piattaforme online. Per quanto qui interessa assumono in particolare rilievo gli artt. 16 e 17 del DSA, sui quali quindi soffermeremo subito la nostra attenzione.

2.1. Meccanismo di *notice and action*

La prima rilevante previsione è quella dell'art. 16 del DSA, che impone a tutti i prestatori di servizi di memorizzazione di predisporre meccanismi di «facile accesso e uso» per «consentire a qualsiasi persona o ente» di notificare la presenza «nel loro servizio

alla base della rimozione delle informazioni dalle relazioni disponibili al pubblico».

[22] G. Buttarelli, *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche*, in *Giornale di diritto amministrativo,* 1, 2023, 116 ss. Autorevole dottrina rileva inoltre come, tra obblighi di diligenza privati e responsabilità pubbliche di *enforcement*, il DSA preveda un sistema "a rete" di poteri di vigilanza e controllo: L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Rivista trimestrale di diritto pubblico*, 4, 2022, 1108.

di informazioni specifiche che tale persona o ente ritiene costituiscano contenuti illegali», con la possibilità di presentare «segnalazioni esclusivamente per via elettronica». Tali operatori, poi, dovranno predisporre misure idonee a facilitare le segnalazioni che appaiano «sufficientemente precise e adeguatamente motivate», qualificandosi in sostanza come tali quelle che presentino una serie di contenuti di dettaglio descritti analiticamente dal par. 2 dell'art. 16[23].

In tale disposizione, poi, il DSA, si occupa di fornire alcune indicazioni ulteriori, sia di carattere più generale che di dettaglio, circa gli obblighi procedurali a carico del prestatore e i diritti previsti per gli utenti interessati.

Dal primo punto di vista, infatti, in parte ricalcando quanto l'art. 14 precisa rispetto alla definizione di termini e condizioni, si prevede l'obbligo per i detti prestatori di prendere in carico simili segnalazioni e di adottare le decisioni in merito alle informazioni cui queste si riferiscono «in modo tempestivo, diligente, non arbitrario e obiettivo», fornendo altresì informazioni specifiche sull'eventuale uso di strumenti automatizzati nel trattare e assumere provvedimenti rispetto alle stesse.

Dal secondo punto di vista, poi, delineando un livello basilare e minimo di "diritti procedurali", si prevede che l'operatore digitale debba informare, sempre «senza indebito ritardo», il segnalatore (che può essere sia una persona fisica che un ente, che abbia fornito il proprio contatto «elettronico») sia del ricevimento della segnalazione, sia della decisione presa in merito, fornendo contestualmente ogni informazione circa i ricorsi disponibili per contestare il provvedimento del prestatore.

È significativo notare, inoltre, come le segnalazioni in questione siano in grado di dispiegare effetti anche rispetto al regime di responsabilità del *provider,* nella misura in cui il paragrafo 3 dell'art. 16 sancisce che, ove tali *notices* consentano all'organizzazione di prendere contezza dell'illegalità del contenuto «senza un esame giuridico dettagliato», «si considera» che queste permettono all'operatore di acquisire una conoscenza effettiva dell'illegalità dell'attività o dell'informazione veicolata tramite i suoi servizi, con tutto ciò che ne consegue a norma dell'art. 6 circa la *hosting provider liability*[24].

La previsione dell'art. 16 è particolarmente opportuna nella misura in cui consente di "istituzionalizzare" un meccanismo di cruciale importanza come quello delle segnalazioni, con cui enti e persone fisiche possono "stimolare" gli operatori digitali a porre in essere in modo più efficace la loro attività di *private enforcement*, anche in un certo sen-

[23] E cioè «a) una spiegazione sufficientemente motivata dei motivi per cui la persona o l'ente presume che le informazioni in questione costituiscano contenuti illegali; b) una chiara indicazione dell'ubicazione elettronica esatta di tali informazioni, quali l'indirizzo o gli indirizzi URL esatti e, se necessario, informazioni supplementari che consentano di individuare il contenuto illegale adeguato al tipo di contenuto e al tipo specifico di servizio di memorizzazione di informazioni; c) il nome e l'indirizzo di posta elettronica della persona o dell'ente che presenta la segnalazione, tranne nel caso di informazioni che si ritiene riguardino uno dei reati di cui agli articoli da 3 a 7 della Direttiva 2011/93/UE (n.d.r. gli illeciti penali relativi agli abusi, allo sfruttamento sessuale dei minori e alla pornografia minorile); d) una dichiarazione con cui la persona o l'ente che presenta la segnalazione conferma la propria convinzione in buona fede circa l'esattezza e la completezza delle informazioni e delle dichiarazioni ivi contenute».

[24] In argomento rinviamo integralmente alla disamina svolta in dettaglio nel primo saggio della presente sezione (di L. D'Agostino, *Disinformazione e obblighi di* compliance *degli operatori del mercato digitale alla luce del nuovo* Digital Services Act). Sul tema v. anche, di recente, S. Braschi, *Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli* Internet Service Provider*?*, in *Diritto penale e processo*, 3, 2023, 367 ss.

so affiancandoli e supportandoli in procedure senz'altro molto onerose già sul piano gestionale e organizzativo. Del resto, *ad impossibilia nemo tenetur*, sicché non potremmo certo aspettarci/pretendere che i soggetti regolati in questione siano in grado, da soli, di identificare ogni contenuto illegale condiviso tramite i loro sevizi.

È molto importante evidenziare, però, come tale meccanismo di *notice and action* debba essere obbligatoriamente predisposto solo per ciò che concerne la segnalazione di attività e contenuti *illegali*[25] e non già, stando alla "lettera" dell'art. 16, per quelli meramente lesivi delle condizioni generali d'uso del servizio o c.d. standard della *community*. Fermo restando che le piattaforme, naturalmente, potranno pur sempre spontaneamente estendere il raggio applicativo di tali procedure, consentendo di attivarle anche per segnalare la presenza di contenuti non illegali, ma semplicemente lesivi delle condizioni d'uso del servizio quanto ad attività che non possono essere svolte sui loro servizi, bisognerebbe forse interrogarsi sulla condivisibilità o meno di tale scelta di regolazione e della decisione del legislatore europeo di non estendere l'adozione obbligatoria di simili procedure anche alle informazioni in parola.

Specie per ciò che concerne il contrasto alla disinformazione, infatti, molto spesso alcune modalità d'utilizzo del servizio (si pensi alla interazione tra più *account* al fine di aumentare artificiosamente la visibilità di certe notizie, o all'uso coordinato di *fake account* o *bot* automatici, etc.) non possono dirsi di per sé – o comunque non possono sempre agevolmente qualificarsi – come illegali; lo stesso vale per molte affermazioni false veicolate in campagne anche coordinate di disinformazione che, secondo quanto abbiamo avuto modo di osservare ampiamente nei precedenti cicli della ricerca, non hanno sovente alcuna rilevanza penale o, in generale, carattere di illiceità per l'ordinamento giuridico[26].

A volte, però, si tratta di informazioni rispetto alle quali la piattaforma può legittimamente decidere di applicare delle restrizioni (da quelle più *soft* concernenti l'utilizzo di *banner* con rinvio ad *alert* di *fact-checkers* indipendenti, fino a misure più incisive come la riduzione di visibilità o la rimozione del contenuto lesivo degli standard della *community*), per cui simili meccanismi di *notice and action* potrebbero rivestire particolare utilità, ferma restando naturalmente la 'generale 'esigenza, sopra evidenziata, che le piattaforme disciplinino l'utilizzo di tale potere "sanzionatorio" nel rispetto dei minimali principi di garanzia propri di qualsiasi paradigma disciplinare/punitivo, anche in ambito privato.

2.2. Obbligo di motivazione sulle misure di moderazione dei contenuti

La seconda previsione della sezione in analisi del DSA (art. 17) riguarda l'obbligo per

[25] Osserva M.L. Bixio, *Gli obblighi applicabili a tutti i prestatori di servizi*, cit., 23, che «la struttura *pyramid base*, tra i diversi tipi di servizi intermediari, ammette solo per l'*hosting* la segnalazione da parte di un soggetto privato e, per conseguenza, l'art. 9 tratta solo degli ordini (e non delle segnalazioni) rivolte ai prestatori di servizi intermediari».

[26] Per ogni riferimento v. E. Birritteri, *Punire la disinformazione*, cit., 316 ss.

i prestatori di *hosting services* di fornire ai destinatari del servizio, salvo che si tratti di contenuti commerciali ingannevoli ad ampia diffusione[27] o dell'esecuzione di ordini di autorità pubbliche *ex* art. 9 DSA, «una motivazione chiara e specifica»[28] su una serie di "sanzioni" applicate in sede di moderazione dei contenuti e nominalmente indicate dal par. 1 della disposizione (dalla semplice riduzione di visibilità dell'informazione, alla sospensione o cessazione della prestazione del servizio, fino alla chiusura dell'*account*)[29].

Il par. 3, inoltre, offre ulteriori e importanti dettagli sul contenuto specifico dell'obbligo di motivazione che grava su simili operatori.

Anzitutto, infatti, occorre chiarire la tipologia di sanzione che è stata irrogata, specificandone la portata territoriale e la durata.

Bisogna, poi, indicare «i fatti e le circostanze su cui si basa la decisione» di applicare la restrizione del servizio, specificando, ma solo «ove opportuno», se la sanzione sia stata applicata all'esito di una segnalazione pervenuta tramite il meccanismo di *notice and action* dell'art. 16 o in virtù di indagini volontarie intraprese di propria iniziativa dall'organizzazione, nonché – ma solo, anche qui, «ove strettamente necessario» – l'identità stessa del notificante. Queste ultime clausole di riserva attribuiscono un notevole margine di apprezzamento alle piattaforme e non potrà che essere l'*enforcement* concreto dal DSA a chiarirne effettivamente la portata. Ci sembra, comunque, si possa leggere tra le righe la volontà del legislatore eurounitario di tutelare i segnalanti, lasciando però agli operatori digitali il delicato compito di operare un complesso bilanciamento tra tali esigenze di protezione e i "diritti di difesa" dell'utente che ha subito la restrizione imposta dalla piattaforma.

Occorre, inoltre, chiarire se la decisione sia stata presa in virtù dell'illegalità del contenuto o della sua incompatibilità con le condizioni generali d'uso del servizio (quindi, con le regole autonormate dalla piattaforma circa i c.d. standard della *community*), in entrambi i casi indicando la specifica base giuridica o la clausola contrattuale "interna" che si assume violata e i motivi per cui l'informazione o il contenuto vengono considerati in contrasto con tali previsioni.

Infine, con ulteriori due indicazioni, come visto, ricorrenti in tutto il DSA, si pre-

---

[27] Qualche chiarimento sul punto è offerto dal considerando 55 del DSA, ove si legge che «L'obbligo di fornire una motivazione non dovrebbe tuttavia applicarsi ai contenuti commerciali ingannevoli ad ampia diffusione diffusi attraverso la manipolazione intenzionale del servizio, in particolare l'utilizzo non autentico del servizio, come l'utilizzo di bot o account falsi o altri usi ingannevoli del servizio».

[28] Il par. 4 della previsione aggiunge che le «Le informazioni fornite dai prestatori di servizi di memorizzazione di informazioni a norma del presente articolo devono essere chiare e facilmente comprensibili e il più possibile precise e specifiche tenuto conto delle circostanze del caso. In particolare le informazioni devono essere tali da consentire ragionevolmente al destinatario del servizio interessato di sfruttare in modo effettivo le possibilità di ricorso di cui al paragrafo 3, lettera f)».

[29] Nello specifico, il par. 1 dell'art. 17 DSA prevede l'obbligo di fornire tale motivazione rispetto alle seguenti misure: «a) eventuali restrizioni alla visibilità di informazioni specifiche fornite dal destinatario del servizio, comprese la rimozione di contenuti, la disabilitazione dell'accesso ai contenuti o la retrocessione dei contenuti; b) la sospensione, la cessazione o altra limitazione dei pagamenti in denaro; c) la sospensione o la cessazione totale o parziale della prestazione del servizio; d) la sospensione o la chiusura dell'account del destinatario del servizio». Si specifica al par. 2, tra l'altro, che tale previsione «si applica solo se le pertinenti coordinate elettroniche sono note al prestatore» e «al più tardi dalla data a partire dalla quale la restrizione è imposta, indipendentemente dal motivo o dal modo in cui è imposta».

vede l'obbligo per il prestatore di chiarire se la decisione sia stata presa utilizzando strumenti automatizzati anche, se del caso, per individuare il contenuto oggetto del provvedimento "sanzionatorio", nonché di fornire «informazioni chiare e di facile comprensione sui mezzi di ricorso a disposizione del destinatario del servizio in relazione alla decisione, in particolare […] attraverso i meccanismi interni di gestione dei reclami, la risoluzione extragiudiziale delle controversie e il ricorso per via giudiziaria». L'art. 17 del DSA riveste, come ben può intuirsi, una primaria importanza rispetto al funzionamento concreto delle dinamiche di *private enforcement* degli operatori digitali.
Infatti, nella fase di autonormazione a monte, come abbiamo rilevato, i soggetti regolati mantengono un significativo margine di apprezzamento nell'individuare le informazioni o i contenuti (anche sul piano della lotta alla disinformazione) che possono essere veicolati o meno tramite le loro piattaforme, al netto della "sintetica" menzione della necessità di esercitare tale potestà di autoregolazione «in modo diligente, obiettivo e proporzionato» e «tenendo debitamente conto dei […] diritti e [delle] libertà fondamentali sanciti dalla Carta». Nella fase di *enforcement* a valle di tali regole autonormate, invece, l'articolo in commento appare più "sensibile" alle esigenze sia di dettagliare maggiormente, e non solo con clausole di carattere generale, gli obblighi degli operatori, sia di rafforzare e specificare con più analiticità i diritti e le garanzie procedurali minime per gli utenti che subiscono simili misure para-punitive[30].
L'ampiezza dell'obbligo motivazionale imposto ai soggetti regolati, infatti, pur ponendo in capo ad essi significativi oneri gestionali e organizzativi, appare una soluzione necessaria in considerazione dei diritti fondamentali su cui simili attività possono significativamente incidere, oltre a fornire una base di informazioni di partenza indispensabile per l'utente che voglia avvalersi degli strumenti di reclamo "interni" o "esterni" effettivamente disponibili a tutela della sua posizione.
In parte qua, allora, e anche tenuto conto del più limitato novero di operatori cui, come visto, si applica tale disposizione, il DSA opera un bilanciamento tutto sommato ragionevole tra tali interessi contrapposti, pure in considerazione del significativo squilibrio tra i "poteri" contrattuali delle parti[31].

3. Disposizioni aggiuntive applicabili alle piattaforme online

Nella struttura a intensità crescente delle *due diligence obligation* del DSA, la sezione III

[30] P. Leerssen, *An end to shadow banning?*, cit., 8, che osserva anche in chiave critica come «*the DSA's approach is inflexible in that it bundles all relevant due process rights – notice, explanation and appeals – into the singular concept of a 'moderation action'. In practice there may be a large set of edge-cases where integral explanation and/or appeal could be onerous in terms of costs, or too sensitive in terms of security, but where a bare notice right could still be of substantial value as a bulwark against shadow banning and as a minimal precondition for legal and social accountability. In this light, the DSA's attempt at balancing is somewhat rudimentary, and in future may benefit from further refinement, such as by incorporating more factors into the shadow banning calculus and unbundling notice safeguards from other aspects of due process*».

[31] Sul problema, in tali contesti, dell"asimmetria delle posizioni' degli attori in campo v. B. Carotti, *La politica europea sul digitale: ancora molto rumore*, in *Rivista trimestrale di diritto pubblico*, 4, 2022, 998. Diffusamente cfr. anche G. Alpa, *Sul potere contrattuale delle piattaforme digitali*, in *Contratto delle imprese*, 2022, 721 ss.

del Capo III del regolamento rafforza ulteriormente gli oneri di *compliance* gravanti sui più importanti *player* del mercato digitale, introducendo una serie di disposizioni aggiuntive applicabili alle piattaforme online, che, come noto, specie nel contrasto alla disinformazione, costituiscono i naturali interlocutori di qualsiasi strategia di regolazione del fenomeno.

Per quanto qui interessa, in particolare, vengono in rilievo le previsioni di cui agli artt. 20, 21 e 22 del DSA, applicabili a tutte le piattaforme online ad eccezione di quelle qualificabili come microimprese o piccole imprese ai sensi della Raccomandazione (CE) 2003/361, per quanto tale deroga non operi rispetto a quelli che, anche tra questi ultimi operatori, vengano designati come «piattaforme online di dimensioni molto grandi a norma dell'articolo 33, indipendentemente dal fatto che si qualifichino come microimprese o piccole imprese»[32].

3.1. Il sistema interno di gestione dei reclami

La prima *due diligence obligation* aggiuntiva per le piattaforme online consiste nell'obbligo di fornire ai propri utenti, comprese persone o enti che presentano una segnalazione, per almeno sei mesi[33] dalla decisione sulla segnalazione o dall'applicazione della "sanzione" nell'ambito dell'attività di moderazione di contenuti illegali o contrari alle condizioni generali del servizio[34], «l'accesso a un sistema interno di gestione dei reclami efficace, che consenta loro di presentare per via elettronica e gratuitamente reclami contro la decisione presa dal fornitore della piattaforma», che sia di «facile accesso e uso» e tale da consentire e agevolare «la presentazione di reclami sufficientemente precisi e adeguatamente motivati».

Anche in questo caso, sulla scorta di quanto già rilevato con riferimento all'art. 14 del DSA in punto di definizione di termini e condizioni del servizio, e in qualche modo a differenza dell'art. 17, il DSA non fornisce un *set* preciso di regole di dettaglio circa il funzionamento specifico di tali procedure interne di reclamo e sui correlati diritti pro-

[32] In particolare, l'art. 19 del DSA stabilisce in dettaglio che «1. La presente sezione, ad eccezione dell'articolo 24, paragrafo 3, non si applica ai fornitori di piattaforme online che si qualificano come microimprese o piccole imprese quali definite nella raccomandazione 2003/361/CE. La presente sezione, ad eccezione dell'articolo 24, paragrafo 3, non si applica ai fornitori di piattaforme online che si sono precedentemente qualificati come microimprese o piccole imprese quali definite nella raccomandazione 2003/361/CE nel corso dei 12 mesi successivi alla perdita di tale qualifica a norma dell'articolo 4, paragrafo 2, della medesima raccomandazione, tranne quando sono piattaforme online di dimensioni molto grandi ai sensi dell'articolo 33. 2. In deroga al paragrafo 1 del presente articolo, la presente sezione si applica ai fornitori di piattaforme online che sono stati designati come piattaforme online di dimensioni molto grandi a norma dell'articolo 33, indipendentemente dal fatto che si qualifichino come microimprese o piccole imprese».

[33] Il par. 2 dell'art. 20 precisa che il «periodo di almeno sei mesi di cui al paragrafo 1 del presente articolo decorre dal giorno in cui il destinatario del servizio è stato informato della decisione a norma dell'articolo 16, paragrafo 5, o dell'articolo 17».

[34] In particolare, il par. 1 dell'art. 20 del DSA menziona: «a) le decisioni che indicano se rimuovere le informazioni o disabilitare l'accesso alle stesse o se limitarne la visibilità; b) le decisioni che indicano se sospendere o cessare in tutto o in parte la prestazione del servizio ai destinatari; c) le decisioni che indicano se sospendere o cessare l'account dei destinatari; d) le decisioni che indicano se sospendere, cessare o limitare in altro modo la capacità di monetizzare le informazioni fornite dai destinatari».

cedurali specie del destinatario della "sanzione" irrogata dalla piattaforma.
Il par. 4 dell'art. 20, invero, si "limita" a sancire l'obbligo delle piattaforme online di gestire i reclami presentati tramite il loro sistema interno in modo «in modo tempestivo, non discriminatorio, diligente e non arbitrario», di ritirare la propria decisione ove il reclamo contenga «sufficienti motivi per indurre il fornitore a ritenere» che la decisione presa sia infondata, di comunicare senza indebito ritardo ai reclamanti la loro «decisione motivata» in merito al reclamo presentato nonché i mezzi ulteriori di ricorso a loro disposizione, nonché – in misura qui forse più significativa – la necessità che il ricorsi interni in questione vengano decisi «con la supervisione di personale adeguatamente qualificato e non avvalendosi esclusivamente di strumenti automatizzati» (essendo, del resto, costante l'attenzione rivolta dal DSA al rispetto dell'art. 22 del GDPR[35]).
Anche qui, dunque, alle piattaforme, fermi restando questi principi di fondo, viene lasciata ampia potestà di disciplinare nel modo ritenuto più opportuno il funzionamento concreto di tali procedure e sistemi interni di reclamo.
Pure in tal caso, però, senza legittimare formalismi eccessivi e non necessari, sarebbe stato auspicabile fornire indicazioni di maggiore dettaglio circa le garanzie procedurali minime a tutela di utenti che si trovino di fronte a decisioni capaci di incidere in modo significativo sui loro diritti fondamentali, avuto naturalmente particolare riguardo, nel settore del contrasto alla disinformazione, alla libertà di espressione.
Nei cicli precedenti della ricerca, del resto, avevamo osservato come proprio le procedure e le regole di funzionamento dei sistemi interni di reclamo fossero un ambito in cui le piattaforme online fanno spesso registrare un ridotto livello di trasparenza, e come fosse necessario costruire una cornice pubblica di regole del gioco tali da obbligare le piattaforme a garantire un livello minimo di "diritti di difesa" a tutela degli utenti, tra cui, ad esempio, il diritto al contraddittorio preventivo, la garanzia di sufficiente autonomia e indipendenza (anche rispetto alla distribuzione interna dei poteri dell'organizzazione) dei soggetti deputati a irrogare la sanzione e a decidere sui connessi reclami, il diritto di richiedere, già a livello interno, un ulteriore riesame della decisione[36].
Pur non potendosi certamente imporre generali modelli standard secondo un analitico livello di dettaglio, insomma, l'impressione anche su questo versante è quella di un percorso che, pur avendo condivisibilmente istituzionalizzato tali meccanismi e correttamente sancito in linea generale l'obbligo delle piattaforme di agire in modo non discriminatorio e arbitrario e secondo diligenza anche nella gestione dei reclami interni, poteva essere ancora perfezionato nella direzione della più efficace tutela dei diritti degli utenti[37].

[35] Sul tema, in generale, dei trattamenti automatizzati anche con riferimento a quest'ultima disposizione, v., nella dottrina penalistica, anche per più ampi riferimenti, tra gli altri: L. D'Agostino, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al d.lgs. 10 agosto 2018, n. 101,* in *Archivio penale,* 1, 17 ss.; G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Diritto penale contemporaneo – Rivista Trimestrale*, 4, 2020, 75 ss.

[36] E. Birritteri, *Punire la disinformazione*, cit., 322 ss.

[37] In dottrina, invero, nei primi commenti al DSA è subito emerso un primo dibattito anche su questi aspetti: cfr. F. G'sell, *The Digital Services Act: A General Assessment*, in A. von Ungern-Sternberg (a cura di), *Content Regulation in the European Union. The Digital Services Act*, Trier, 2023, 95.

3.2. La risoluzione extragiudiziale delle controversie

L'art. 21 del DSA stabilisce che gli utenti e coloro che hanno presentato segnalazioni hanno il diritto di scegliere, rispetto a qualsiasi controversia inerente alle stesse decisioni delle piattaforme menzionate dal par. 1 dell'art. 20 del DSA, compresi i «reclami che non è stato possibile risolvere mediante il sistema interno di gestione dei reclami di cui a tale articolo», «qualunque organismo di risoluzione extragiudiziale delle controversie» certificato ai sensi del par. 3 dell'art. 21, che subordina l'ottenimento di tale certificazione, attribuita dal coordinatore dei servizi digitali dello Stato membro, al soddisfacimento di requisiti dettagliatamente descritti e volti principalmente ad assicurare la competenza, l'imparzialità e l'indipendenza di simili organismi e l'adozione da parte loro di «regole procedurali chiare ed eque»[38].

I fornitori di piattaforme online hanno l'obbligo di rendere edotti chiaramente i propri utenti sulle possibilità di avere accesso a tali strumenti di risoluzione extragiudiziale delle controversie, facendo sì che tali informazioni siano «agevolmente accessibili sulla loro interfaccia online», pur restando impregiudicato, ai sensi del par. 1 dell'art. 21, «il diritto del destinatario del servizio in questione di avviare, in qualsiasi fase, procedi-

[38] In particolare, il par. 3 dell'art. 21 del DSA prevede che «Il coordinatore dei servizi digitali dello Stato membro in cui è stabilito l'organismo di risoluzione extragiudiziale delle controversie certifica tale organismo, su sua richiesta, per un periodo massimo di cinque anni rinnovabile, se il medesimo ha dimostrato di soddisfare tutte le condizioni seguenti: a) è imparziale e indipendente, anche sul piano finanziario, dai fornitori di piattaforme online e dai destinatari del servizio prestato dai fornitori di piattaforme online, ivi compresi le persone o gli enti che hanno presentato segnalazioni; b) dispone delle competenze necessarie, in relazione alle questioni che sorgono in uno o più ambiti specifici relativi ai contenuti illegali o in relazione all'applicazione e all'esecuzione delle condizioni generali di uno o più tipi di piattaforme online, per consentire a tale organismo di contribuire efficacemente alla risoluzione di una controversia; c) i suoi membri sono retribuiti secondo modalità non legate all'esito della procedura; d) la risoluzione extragiudiziale delle controversie che offre è facilmente accessibile attraverso le tecnologie di comunicazione elettronica e prevede la possibilità di avviare la risoluzione delle controversie e di presentare i necessari documenti giustificativi online; e) è in grado di risolvere le controversie in modo rapido, efficiente ed efficace sotto il profilo dei costi e in almeno una delle lingue ufficiali delle istituzioni dell'Unione; f) la risoluzione extragiudiziale delle controversie che offre avviene secondo regole procedurali chiare ed eque che sono facilmente e pubblicamente accessibili e conformi al diritto applicabile, compreso il presente articolo. Ove opportuno il coordinatore dei servizi digitali specifica nel certificato: a) le questioni concrete cui si riferisce la competenza dell'organismo, a norma del primo comma, lettera b); e b) la lingua o le lingue ufficiali delle istituzioni dell'Unione in cui l'organismo è in grado di risolvere le controversie, a norma del primo comma, lettera e)». Il par. 4 della medesima previsione aggiunge che «I coordinatori dei servizi digitali elaborano ogni due anni una relazione sul funzionamento degli organismi di risoluzione extragiudiziale delle controversie da essi certificati. In particolare, tale relazione: a) elenca il numero di controversie che ciascun organismo di risoluzione extragiudiziale delle controversie certificato ha ricevuto ogni anno; b) indica l'esito delle procedure avviate dinanzi a tali organi e il tempo medio necessario per risolvere le controversie; c) individua e spiega eventuali carenze sistemiche o settoriali o difficoltà incontrate in relazione al funzionamento di tali organismi; d) individua le migliori prassi relative a tale funzionamento; e) formula raccomandazioni su come migliorare tale funzionamento, ove opportuno». Si vedano altresì i parr. 6, 7, 8 e 9 dell'art. 21 che prevedono rispettivamente: a) la possibilità per gli Stati membri di istituire organismi di risoluzione extragiudiziale delle controversie o di sostenere l'attività di quelli che hanno certificato; b) la possibilità di revocare la certificazione ove vengano meno le condizioni di cui al par. 3, assicurando un contraddittorio preventivo prima di dar corso alla decisione; c) l'obbligo per il coordinatore dei servizi digitali di comunicare alla Commissione gli organismi certificati; d) il fatto che l'art. 21 lasci «impregiudicati la direttiva 2013/11/UE e le procedure e gli organismi di risoluzione alternativa delle controversie per i consumatori istituiti a norma di tale direttiva».

menti per contestare tali decisioni da parte dei fornitori di piattaforme online dinanzi a un organo giurisdizionale conformemente al diritto applicabile».
Del resto, la disposizione è ben chiara nel prevedere che tali organismi di risoluzione extragiudiziale non abbiano il potere di imporre una decisione «vincolante per le parti» e che le stesse piattaforme online possano legittimamente rifiutarsi di adirli «qualora una controversia riguardante le stesse informazioni e gli stessi motivi di presunta illegalità o incompatibilità dei contenuti sia già stata risolta».
Sul piano procedurale, si prevede che le parti «adiscono in buona fede» l'organismo in questione, che deve mettere a loro disposizione[39] il proprio provvedimento, come visto, non vincolante, entro 90 giorni dal ricevimento del reclamo, con la possibilità di prorogare il termine per definire il procedimento di oltre 90 giorni al massimo in caso di controversie molto complesse.
Per ciò che concerne i risarcimenti e i costi della lite, tra l'altro, è evidente il *favor* legislativo nei confronti del reclamante, alla luce del noto squilibrio contrattuale e di poteri tra le parti in causa in questi contesti, specie nella misura in cui si prevede che gli utenti debbano poter accedere «gratuitamente, o per un importo simbolico» a tali meccanismi[40], nonché che, a differenza delle piattaforme, non debbano farsi carico dei e «diritti e [del]le altre spese che il fornitore della piattaforma online ha sostenuto o deve sostenere in relazione alla risoluzione della controversia, a meno che l'organismo di risoluzione extragiudiziale delle controversie non ritenga che detto destinatario abbia agito manifestamente in mala fede».
Tale previsione, al netto della natura non vincolante delle decisioni degli organismi in parola, ci pare rivesta in definitiva una indubbia importanza nella misura in cui offre agli utenti dei servizi digitali una ulteriore alternativa per tutelare la propria posizione, specie lì dove il sistema di reclamo interno alla piattaforma online non abbia dato gli esiti sperati o comunque presenti criticità, senza dover necessariamente adire l'autorità giudiziaria o in generale gli attori pubblici di *enforcement* e senza che l'innesco di tale binario alternativo di risoluzione delle controversia pregiudichi il diritto di poter percorrere comunque, in qualsiasi fase, le "strade" della giurisdizione statale.
Ciò potrà comportare benefici anche per gli stessi operatori digitali e, soprattutto, per la gestione statale dei servizi giudiziari, nella misura in cui tali ADR, se correttamente implementate, possono aiutare gli Stati a raggiungere l'obiettivo di gestire in modo più efficiente la macchina della giustizia, non aumentando la mole (in molti Paesi già considerevole) dei contenziosi[41].

[39] Il par. 5 dell'art. 21 prevede altresì che prima «di avviare la risoluzione delle controversie, gli organismi di risoluzione extragiudiziale delle controversie certificati comunicano al destinatario del servizio, ivi compresi le persone o gli enti che hanno presentato una segnalazione, e al fornitore della piattaforma online interessata i diritti o i meccanismi utilizzati per determinarli».

[40] Che si rifanno alla logica delle *alternative dispute resolution* (ADR).

[41] Per un commento a queste previsioni del DSA in tema di risoluzione alternativa delle controversie, nonché per una disamina del loro impatto sulla nostra legislazione nazionale in tema di ADR, v. G. Gioia - A. Bigi, *La risoluzione stragiudiziale delle controversie nel mercato dei servizi digitali (artt. 17, 20, 21, 24, 35 – Capo III, Sezioni 2, 3 e 5)*, in *Diritto di internet*, 1, 2023, 39 ss. V. altresì A.M. Felicetti, *La risoluzione extragiudiziale delle dispute nei mercati digitali: alcune novità dall'Europa*, in *Rivista trimestrale di diritto e procedura civile*, 1, 2023, 197 ss.

3.3. Le previsioni in tema di segnalatori attendibili

L'art. 22 del DSA prevede l'obbligo per le piattaforme online di adottare «le misure tecniche e organizzative necessarie» per trattare con priorità e decidere «senza indebito ritardo» le segnalazioni circa la presenza di contenuti illegali presentate, tramite il meccanismo di *notice and action* di cui all'art. 16, da «segnalatori attendibili» entro «il loro ambito di competenza designato».

In particolare, la qualifica di segnalatore attendibile viene riconosciuta, a richiesta di qualunque ente, dal coordinatore dei servizi digitali «dello Stato membro in cui è stabilito il richiedente», a condizione che quest'ultimo dimostri di soddisfare una serie di condizioni specificamente indicate dal par. 2 dell'art. 22 e tese a garantire, tra l'altro, l'indipendenza, la particolare *expertise* e la diligenza di tali *trusted flaggers*[42], i quali, tra l'altro, devono pubblicare relazioni almeno annuali sulle loro attività[43] e possono vedersi revocata la qualifica di segnalatori attendibili, anche su istanza delle piattaforme online, ove abbiano presentato un numero significativo di segnalazioni infondate o, comunque, in generale, ove siano venute meno le condizioni stabilite dal paragrafo 2[44].

---

[42] In particolare, il par. 2 dell'art. 22 del DSA stabilisce che «La qualifica di «segnalatore attendibile» a norma del presente regolamento viene riconosciuta, su richiesta di qualunque ente, dal coordinatore dei servizi digitali dello Stato membro in cui è stabilito il richiedente al richiedente che abbia dimostrato di soddisfare tutte le condizioni seguenti: a) dispone di capacità e competenze particolari ai fini dell'individuazione, dell'identificazione e della notifica di contenuti illegali; b) è indipendente da qualsiasi fornitore di piattaforme online; c) svolge le proprie attività al fine di presentare le segnalazioni in modo diligente, accurato e obiettivo».

[43] Il par. 3 dell'art. 22 del DSA prevede specificamente che «I segnalatori attendibili pubblicano, almeno una volta all'anno, relazioni facilmente comprensibili e dettagliate sulle segnalazioni presentate conformemente all'articolo 16 durante il periodo di riferimento. La relazione elenca almeno il numero di segnalazioni classificate in base: a) all'identità del prestatore di servizi di memorizzazione di informazioni; b) al tipo di presunto contenuto illegale notificato; c) alle azioni adottate dal prestatore. Tali relazioni includono una spiegazione delle procedure in atto per assicurare che il segnalatore attendibile mantenga la propria indipendenza. I segnalatori attendibili inviano tali relazioni al coordinatore dei servizi digitali che ha conferito la qualifica e le mettono a disposizione del pubblico. Le informazioni in tali relazioni non contengono dati personali». Inoltre, ai sensi dei parr. 4, 5 e 8 dell'art. 22 in commento i coordinatori dei servizi digitali devono comunicare alla Commissione – la quale predisporrà una banca dati accessibile al pubblico con l'elenco di tutti i segnalatori attendibili e potrà emanare, se necessario, «orientamenti per assistere i fornitori di piattaforme online e i coordinatori dei servizi digitali nell'applicazione dei paragrafi 2, 6 e 7» – ogni provvedimento relativo al riconoscimento o alla sospensione/revoca della qualifica di segnatore attendibile.

[44] I parr. 6 e 7 dell'art. 22 del DSA, invero, sanciscono che «6. Se un fornitore di piattaforme online dispone di informazioni indicanti che un segnalatore attendibile ha presentato un numero significativo di segnalazioni non sufficientemente precise, inesatte o non adeguatamente motivate avvalendosi dei meccanismi di cui all'articolo 16, comprese le informazioni raccolte in relazione al trattamento dei reclami tramite i sistemi interni di gestione dei reclami di cui all'articolo 20, paragrafo 4, comunica dette informazioni al coordinatore dei servizi digitali che ha riconosciuto la qualifica di segnalatore attendibile all'ente interessato, fornendo le spiegazioni e i documenti giustificativi necessari. Una volta ricevute le informazioni dal fornitore delle piattaforme online e ove il coordinatore dei servizi digitali ritenga che vi siano motivi legittimi per avviare un'indagine, la qualifica di segnalatore attendibile è sospesa durante il periodo dell'indagine. Tale indagine è condotta senza indebiti ritardi. 7. Il coordinatore dei servizi digitali che ha riconosciuto la qualifica di segnalatore attendibile a un ente revoca tale qualifica se accerta, a seguito di un'indagine avviata di propria iniziativa o in base a informazioni ricevute da terzi, comprese le informazioni fornite da un fornitore di piattaforme online a norma del paragrafo 6, che l'ente non soddisfa più le condizioni di cui al paragrafo 2. Prima di revocare tale qualifica, il coordinatore dei servizi digitali dà all'ente in questione la possibilità di rispondere alle constatazioni della sua indagine e di reagire

Il considerando 61 del DSA fornisce interessanti chiarimenti circa le particolari figure cui il decisore pubblico europeo ha evidentemente pensato nel costruire tale disposizione, specificando che può trattarsi sia di enti di natura pubblica (ad es. Europol o le unità addette alle segnalazioni di contenuti terroristici su internet) sia di organismi privati (ad es. gli enti facenti parte della «rete di linee di emergenza per la segnalazione di materiale pedopornografico INHOPE e le organizzazioni impegnate nella notifica dei contenuti razzisti e xenofobi illegali online»), indicando tra l'altro l'importanza, per «evitare di attenuare il valore aggiunto di tale meccanismo», di «limitare il numero complessivo di qualifiche» conferite in conformità al DSA.
La decisione del legislatore eurounitario, in definitiva, è quella di obbligare le piattaforme online a predisporre una sorta di canale di segnalazione privilegiato per tali enti, nella convinzione che questi possano supportare in modo particolarmente efficace questi operatori digitali nelle loro attività di "*digital patrolling*", secondo un approccio improntato alla cooperazione tra i vari *stakeholder* che, come noto, ha rivestito e riveste grande importanza nella lotta alle campagne (coordinate e non) di disinformazione[45].

4. Gli obblighi supplementari a carico delle *Very Large Online Platforms (VLOPs)* e dei *Very Large Online Search Engines (VLOSEs)*: la scommessa del legislatore europeo sulla compliance

La sezione V del Capo III del DSA corrisponde al "gradino" più elevato del sistema di *due diligence obligation* a livelli di intensità crescente costruito dal nuovo regolamento europeo, rivolgendosi ai motori di ricerca e alle piattaforme online di "dimensioni molto grandi", qualificandosi in questo modo gli operatori che vengono espressamente designati come tali da una decisione della Commissione europea[46], a norma dell'art.

alla sua intenzione di revocarne la qualifica di segnalatore attendibile».

[45] Per una panoramica dei vari approcci in materia di contrasto alla disinformazione v. O. Pollicino, *The European approach to disinformation: comparing supranational and national measures*, in *Annuario di diritto comparato e di studi legislativi*, 1, 2020, 175 ss. In generale, sulle dinamiche di co-regolazione pubblico-privato che riguardano le piattaforme v. ampiamente A. Simoncini, *La co-regolazione delle piattaforme digitali*, in *Rivista trimestrale di diritto pubblico*, 4, 2022, 1031 ss.

[46] L'art. 24 del DSA impone invero alle piattaforme online e ai motori di ricerca di pubblicare nella loro interfaccia online e comunicare al coordinatore dei servizi digitali del luogo di stabilimento e alla Commissione, su loro richiesta, le informazioni sul numero medio mensile di destinatari attivi del servizio, calcolato in conformità alle metodologie stabilite con atti delegati dalla Commissione stessa, fermo restando che, ai sensi dell'art. 33, la Commissione può comunque adottare la decisione circa la designazione di tali operatori come piattaforme o motori di ricerca 'di dimensioni molto grandi' sulla base di «qualsiasi altra informazione a sua disposizione», dovendo tuttavia in quest'ultimo caso garantire al *provider* una sorta di contradditorio preventivo, dandogli la possibilità di presentare il proprio parere in merito a tale decisione entro dieci giorni lavorativi. Si prevede, inoltre, che la Commissione adotti tali decisioni «previa consultazione dello Stato membro di stabilimento o tenuto conto delle informazioni fornite dal coordinatore dei servizi digitali del luogo di stabilimento a norma dell'articolo 24, paragrafo 4». La Commissione, infine, deve pubblicare sulla Gazzetta Ufficiale dell'Unione europea, e costantemente aggiornare, l'elenco degli operatori qualificati 'di dimensioni molto grandi', potendo porre fine alla designazione del *provider* come tale ove successivamente quest'ultimo non soddisfi più tale requisito quantitativo.

33 DSA, con riferimento a coloro «che hanno un numero medio mensile di destinatari attivi[47] del servizio nell'Unione pari o superiore a 45 milioni».

Si tratta, per così dire, dei *target* più importanti della strategia di regolazione del legislatore eurounitario, rispetto ai quali il DSA riserva incisivi poteri di *enforcement* (esercitati direttamente, tra l'altro, avuto riguardo a tale sezione del regolamento, dalla Commissione europea, così da "contrapporre" un interlocutore sovranazionale "di peso" a società, esse stesse, multinazionali e detentrici di rilevanti poteri[48]), nonché i più significativi obblighi di conformità che si aggiungono, come sappiamo, a quelli delle sezioni del regolamento precedentemente analizzate.

Tra tali operatori, del resto, si collocano i più importanti *social network* (tra gli altri, Facebook e Twitter, in base alla prima *designation decision* resa pubblica dalla Commissione)[49] che, nel contrasto alla disinformazione, esercitano un ruolo assolutamente decisivo e che devono essere necessariamente chiamati dal decisore pubblico a svolgere un ruolo proattivo, come abbiamo cercato di argomentare già nei precedenti cicli della ricerca[50].

Ed è proprio quest'ultimo obiettivo quello che il DSA tenta qui di raggiungere, tramite una scelta di *policy* ben precisa: quella di puntare sugli stilemi, sui paradigmi, sugli strumentari ormai classici dell'era della *corporate compliance*, già sperimentati in qualche misura in altri regolamenti europei (spicca su tutti ovviamente, per importanza e contiguità con il DSA, il *General Data Protection Regulation*)[51].

Come subito vedremo, peraltro, il legislatore eurounitario sembra scommettere su tale scelta di politica del diritto in modo ancor più deciso, disciplinando con un particolare livello di dettaglio, per quanto qui interessa, i criteri di valutazione e gestione dei rischi, l'architettura dei sistemi e delle metodologie di controllo interno, i meccanismi di cooperazione pubblico-privato specie nella risposta alle crisi.

Si entra qui, insomma, nel "cuore pulsante" del regolamento, che ha a che fare con la gestione e la mitigazione dei "*systemic risks*" degli ambienti digitali moderni – per ciò che concerne, tra l'altro, i diritti fondamentali, la libertà di espressione, il pluralismo dei

---

[47] L'art. 3 del DSA fornisce, alle lett. p) e q), le seguenti definizioni: «p) «destinatario attivo di una piattaforma online»: il destinatario del servizio che si è avvalso di una piattaforma online richiedendo alla piattaforma online di ospitare informazioni o esponendosi alle informazioni ospitate dalla piattaforma online e diffuse attraverso la sua interfaccia online; q) «destinatario attivo di un motore di ricerca online»: il destinatario del servizio che ha formulato una richiesta a un motore di ricerca online e si è esposto a informazioni indicizzate e presentate sulla sua interfaccia online».

[48] Cfr. nel dettaglio, anche per ogni ulteriore riferimento, il tezo saggio della presente sezione (di R. Sabia, *L'*enforcement *pubblico del* Digital Services Act *tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni*). Che si tratti degli interlocutori più importanti in qualche misura è "dimostrato" anche dal fatto che ai sensi dell'art. 43 DSA la Commissione europea «addebita ai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi un contributo annuale per le attività di vigilanza al momento della loro designazione a norma dell'articolo 33».

[49] In conformità al DSA, il 25 aprile 2023 la Commissione ha già provveduto a designare come di "dimensioni molto grandi" 2 motori di ricerca (Bing e Google Search) e 17 piattaforme (Alibaba AliExpress; Amazon Store; Apple AppStore; Booking.com; Facebook; Google Play; Google Maps; Google Shopping; Instagram; LinkedIn; Pinterest; Snapchat; TikTok; Twitter; Wikipedia; YouTube; Zalando): cfr. *europa.eu/commission*.

[50] V. *supra* par. 1 per tutti i necessari rinvii. In argomento v. anche, da ultimo, le considerazioni di V. Zeno-Zencovich, *The EU regulation of speech. A critical view*, in questa *Rivista*, 1, 2023, 14.

[51] Da ultimo, per un confronto tra DSA e GDPR, v., anche per ogni ulteriore approfondimento, M. Iaselli, Digital Services Act *e* Privacy, in *Diritto di internet*, 1, 2023, 67 ss.

media, i diritti dei minori, l'integrità dei processi elettorali, la salute e la sicurezza pubblica – la cui valutazione e mitigazione viene affidata agli stessi operatori che generano simili rischi e alle dinamiche di cooperazione istituzionalizzata tra pubblico-privato, secondo modelli di regolazione, appunto, ormai consolidati in vari ordinamenti e in diversi settori di disciplina (si pensi all'ambiente, alla sicurezza sul lavoro, alla *privacy*)[52].

4.1. Obblighi di *risk assessment*

La prima *due diligence obligation* aggiuntiva per i detti operatori di "dimensioni molto grandi" riguarda l'obbligo di effettuare almeno una volta all'anno, nonché «in ogni caso prima dell'introduzione di funzionalità che possono avere un impatto critico», un *assessment* concernente l'individuazione, l'analisi e la valutazione «con diligenza» degli eventuali «rischi sistemici» derivanti dalla progettazione, dal funzionamento o dall'uso dei loro servizi e dei relativi sistemi (anche algoritmici).
L'art. 34 del DSA esige un'analisi specifica «e proporzionata ai rischi sistemici, tenendo in considerazione la loro gravità e la loro probabilità», che comprenda i seguenti "*systemic risks*": *a)* la diffusione di contenuti illegali tramite il proprio servizio; *b)* «eventuali effetti negativi, attuali o prevedibili» collegati alla propria attività e relativi all'esercizio di diritti fondamentali tra cui, tra l'altro, la tutela dei dati personali, la libertà di espressione e di informazione, inclusi il pluralismo dei media, la non discriminazione, i diritti del minore, la tutela dei consumatori[53]; *c)* eventuali effetti negativi «sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica»; *d)* qualsiasi incidenza non positiva 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».
Si tratta, a ben vedere, non solo dei principali ambiti rispetto ai quali diversi *social media* già disciplinano *policy* interne più o meno articolate[54], ma anche di alcuni degli interessi sui quali la *misinformation* e le azioni (coordinate e non) di disinformazione possono più significativamente incidere, con la conseguenza che inevitabilmente piattaforme online e motori di ricerca "*very large*" saranno chiamati, secondo la predetta cadenza periodica, ad autovalutare attentamente il rischio che simili comportamenti possano essere compiuti nell'ambito dei propri servizi e, come vedremo tra poco[55], a farsi carico del delicato compito di introdurre misure per mitigare questi potenziali effetti negativi. Lo stesso considerando 84 del DSA, del resto, chiarisce come tali fornitori dovrebbero

[52] V., per tutti, A. Gullo, voce *Compliance*, in G. Mannozzi - C. Perini - F. Consulich - C. Piergallini - M. Scoletta - C. Sotis (a cura di), *Studi in onore di Carlo Enrico Paliero*, Milano, 2022, 1289 ss.

[53] Nel dettaglio, l'art. 34, par. 1, lett. b) del DSA si riferisce a «eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali, in particolare i diritti fondamentali alla dignità umana sancito nell'articolo 1 della Carta, al rispetto della vita privata e familiare sancito nell'articolo 7 della Carta, alla tutela dei dati personali sancito nell'articolo 8 della Carta, alla libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, sanciti nell'articolo 11 della Carta, e alla non discriminazione sancito nell'articolo 21 della Carta, al rispetto dei diritti del minore sancito nell'articolo 24 della Carta, così come all'elevata tutela dei consumatori, sancito nell'articolo 38 della Carta».

[54] Abbiamo effettuato un'analisi di dettaglio di queste politiche in E. Birritteri, *Punire la disinformazione*, cit., 304 ss.

[55] Cfr. il paragrafo successivo.

«prestare particolare attenzione al modo in cui i loro servizi sono utilizzati per diffondere o amplificare contenuti fuorvianti o ingannevoli, compresa la disinformazione».
Molto opportunamente, poi, il par. 2 dell'art. 34 del DSA detta ulteriori criteri per "guidare" e orientare correttamente tale *risk assessment*, nella misura in cui si esige che la valutazione in questione tenga conto «in particolare, dell'eventualità e del modo in cui i seguenti fattori influenzano uno dei rischi sistemici di cui al paragrafo 1: a) la progettazione dei loro sistemi di raccomandazione e di qualsiasi altro sistema algoritmico pertinente; b) i loro sistemi di moderazione dei contenuti; c) le condizioni generali applicabili e la loro applicazione; d) i sistemi di selezione e presentazione delle pubblicità; e) le pratiche del fornitore relative ai dati […]; [la] manipolazione intenzionale del loro servizio, anche mediante l'uso non autentico o lo sfruttamento automatizzato del servizio, nonché l'amplificazione e la diffusione potenzialmente rapida e ampia di contenuti illegali e di informazioni incompatibili con le condizioni generali»[56].
La centralità di questi aspetti, nel contrasto alla disinformazione, è di palmare evidenza. Anche nel corso dei precedenti cicli della ricerca[57], infatti, avevamo osservato come alcune caratteristiche specifiche del modello di business di tali *Big Tech* siano in grado di favorire la diffusione dei possibili effetti negativi che la condivisione di notizie false online può generare su interessi come l'integrità dei processi e delle consultazioni elettorali, la salute pubblica (si pensi alle molte informazioni false condivise in relazione al Covid-19), il pluralismo dei media. Ad esempio, come noto, i sistemi di raccomandazione tendono a riproporre all'utente contenuti sempre più in linea con la propria precedente attività in rete, con la conseguenza di innescare un continuo "bombardamento" nei suoi riguardi di contenuti falsi che lo hanno già in precedenza interessato – e che rischiano così di divenire rapidamente virali in rete con tutto ciò che di negativo può derivarne – o di *post* potenzialmente molto pericolosi per il suo benessere psicofisico (si pensi a utenti che tendono ad essere attratti, per uno stato depressivo, da informazioni relative ad atti di autolesionismo). Si può far riferimento, altresì, alle tecniche di manipolazione intenzionale del servizio (tra cui l'interazione artificiosa tra più *account* per aumentare in modo fraudolento la visibilità di certe notizie, o l'uso agli stessi fini di *bot* automatici e profili *fake*) spesso utilizzati in campagne coordinate di disinformazione. Ancora, palese è il richiamo, nel riferimento da parte dell'art. 34 del DSA alle modalità di moderazione dei contenuti e alla definizione delle condizioni generali d'uso del servizio, al rischio che una non equilibrata politica di articolazione di simili *policy* interne finisca per risolversi in una illegittima censura nell'ambito del libero confronto politico, e, in generale, in una forma di illecita interferenza sulla libertà di espressione di personaggi pubblici e cittadini.
Di qui l'impatto di tali realtà digitali sui menzionati diritti fondamentali e la necessità

[56] Si prevede altresì che «La valutazione tiene conto di specifici aspetti regionali o linguistici, anche laddove siano specifici di uno Stato membro. 3 I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi conservano i documenti giustificativi delle valutazioni dei rischi per almeno tre anni dopo l'esecuzione delle valutazioni dei rischi e, su richiesta, li comunicano alla Commissione e al coordinatore dei servizi digitali del luogo di stabilimento».

[57] Cfr. *supra*, par. 1, per tutti i necessari rinvii rispetto ai temi qui di seguito menzionati. Ampiamente su tali profili v. recentemente A. Manganelli - A. Nicita, *Regulating Digital Markets. The European Approach*, Cham, 2022, 177 ss.

per le organizzazioni in questione di autovalutare con attenzione tali risvolti potenzialmente "perversi" dei loro sistemi e servizi.
Si tratta di una norma chiave che si pone l'obiettivo di sensibilizzare le piattaforme sull'esigenza di farsi carico degli interessi di tutti gli *stakeholder* che possono in qualche misura essere influenzati dalla loro attività, non potendo le esigenze di *business* e di profitto essere perseguite a discapito di tali diritti individuali e beni collettivi[58]. Ciò secondo un approccio sistematico e sfruttando la capacità organizzativa e di gestione di modelli di *compliance* e metodologie di analisi del rischio che simili grandi *corporation* certamente possiedono[59].
Sotto tale profilo, allora, ci pare che questa disposizione detti una condivisibile cornice pubblicistica di riferimento per una attività di *risk assessment* che appare oggi indispensabile e che, pur ponendo un significativo onere organizzativo e gestionale in capo a tali attori, sembra proporzionata alla loro "potenza di fuoco" sul mercato globale e un bilanciamento tutto sommato più che ragionevole tra i vari interessi contrapposti[60].
L'auspicio dei regolatori, tra l'altro, è che la possibilità per i soggetti regolati di essere esposti, in caso di non conformità con tali obblighi di *due diligence*, a sanzioni e meccanismi di *enforcement* potenzialmente molto efficaci[61], certamente stimolerà le c.d. VLOPs (*Very Large Online Platforms*) e i c.d. VLOSEs (*Very Large Online Search Engines*) ad effettuare tali valutazioni con serietà e significativo impegno, scongiurando la possibilità di legittimare forme di c.d. mera *cosmetic* o *paper compliance*[62].

4.2. Le previsioni in punto di mitigazione dei rischi

Il DSA disciplina naturalmente anche la fase conseguente al *risk assessment* effettuato ai sensi dell'art. 34, richiedendo alle piattaforme online e ai motori di ricerca di dimensioni molto grandi l'adozione di «misure di attenuazione ragionevoli, proporzionate ed efficaci, adattate ai rischi sistemici specifici individuati a norma dell'articolo 34, prestando particolare attenzione agli effetti di tali misure sui diritti fondamentali».
L'art. 35 contempla un elenco molto fitto di alcune possibili "*mitigation measures*", strettamente interconnesse agli ambiti di rischio identificati dall'art. 34, tra cui: l'adeguamento di progettazione, caratteristiche e funzionamento dei servizi, condizioni genera-

[58] Su tale esigenza con specifico riguardo alla lotta alla disinformazione v. ampiamente P. Severino, voce *Disinformazione*, in G. Mannozzi - C. Perini - F. Consulich - C. Piergallini - M. Scoletta - C. Sotis (a cura di), *Studi in onore di Carlo Enrico Paliero*, Milano, 2022, 1373 ss.

[59] In generale, sul tema dell'articolazione della *compliance* nelle realtà multinazionali, v. da ultimo in dettaglio S. Manacorda, *The "Dilemma" of Criminal Compliance for Multinational Enterprises in a Fragmented Legal Word*, in S. Manacorda - F. Centonze (a cura di), *Corporate Compliance on a Global Scale*, Cham, 2022, 67 ss. Sul punto v. anche V. Mongillo, *Presente e futuro della* compliance *penale*, in *sistema penale.it*, 11 gennaio 2022.

[60] In generale, sull'approccio del DSA in punto di bilanciamento tra i vari interessi contrapposti, v. G. Caggiano, *La proposta di* Digital Services Act *per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in *Annali AISDUE*, 1, 2021, 28.

[61] Cfr. ancora il terzo saggio della presente sezione monografica.

[62] Su tale nozione v., per tutti, V. Mongillo, *La responsabilità penale tra individuo ed ente collettivo*, Torino, 2018, 187 e 471.

li e correlato *enforcement*, sistemi algoritmici, di raccomandazione e pubblicità, interfacce online; misure di sensibilizzazione e l'adeguamento «delle procedure di moderazione dei contenuti, compresa la velocità e la qualità del trattamento delle segnalazioni concernenti tipi specifici di contenuti illegali e, se del caso, la rapida rimozione dei contenuti oggetto della notifica o la disabilitazione dell'accesso agli stessi, in particolare in relazione all'incitamento illegale all'odio e alla violenza online, nonché l'adeguamento di tutti i processi decisionali pertinenti e delle risorse dedicate alla moderazione dei contenuti»[63]; l'avvio o l'adeguamento della cooperazione con i *trusted flaggers* e l'attuazione delle decisioni degli organismi di risoluzione extragiudiziale delle controversie; la cooperazione con altre piattaforme o motori di ricerca sulla base di codici di condotta e protocolli di crisi *ex* art. 45 e 48 del DSA; misure a tutela dei minori come «strumenti di verifica dell'età e di controllo parentale, o strumenti volti ad aiutare i minori a segnalare abusi o ottenere sostegno»; misure specifiche afferenti, in sostanza, al fenomeno dei cc.dd. *deep fake*[64].

Al di là di alcune indicazioni di maggiore dettaglio (ad es. in tema di azioni a tutela dei minori e di contrasto, come visto da ultimo, ai *deep fake*), quindi, il DSA menziona soltanto, per così dire, le macro-tipologie di misure che le piattaforme possono autonormare e adottare al fine di gestire e mitigare i rischi connessi all'impatto dei loro servizi sui detti diritti fondamentali e interessi individuali e collettivi. Ci si riferisce, insomma, all'adeguamento di certe *policy* o determinati processi, ma non si forniscono indicazioni più precise e puntuali su *come farlo*, sulle specifiche misure adottabili per conseguire l'obiettivo di risolvere le criticità delle procedure individuate in sede di valutazione del rischio. Il regolatore europeo, in linea con quanto si è visto accade anche rispetto ad altre disposizioni del regolamento, è sempre ben attento a non imporre agli operatori digitali particolari e dettagliate politiche sull'organizzazione e la gestione operativa dei loro servizi, lasciando loro, anche in tale sede, un ampio margine di apprezzamento.

La convinzione pare essere quella dell'impossibilità o comunque dell'inopportunità di fornire procedure e modelli di gestione "preconfezionati", positivizzando analiticamente le cautele imposte, e della necessità, piuttosto, di lasciare liberi i soggetti regolati di costruire autonomamente le proprie "regole interne" secondo una logica *taylor made*, fornendo indicazioni di scopo di carattere generale e qui, in qualche misura, anche una metodologia di analisi e un elenco di possibili contromisure e ambiti di rischio specifici da considerare, menzionando soltanto il *genus* di riferimento delle varie possibili "*effective mitigation measures*"[65].

---

[63] La lett. f) del par. 1 dell'art. 35 del DSA menziona anche, in generale, «il rafforzamento dei processi interni, delle risorse, della sperimentazione, della documentazione o della vigilanza sulle loro attività, in particolare per quanto riguarda il rilevamento dei rischi sistemici».

[64] In particolare, ai sensi dell'art. 35, par. 1, lett. k) del DSA, si tratta del «il ricorso a un contrassegno ben visibile per fare in modo che un elemento di un'informazione, sia esso un'immagine, un contenuto audio o video, generati o manipolati, che assomigli notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che a una persona appaia falsamente autentico o veritiero, sia distinguibile quando è presentato sulle loro interfacce online e, inoltre, la fornitura di una funzionalità di facile utilizzo che consenta ai destinatari del servizio di indicare tale informazione». Per un recente approfondimento del tema cfr. M. Cazzaniga, *Una nuova tecnica (anche) per veicolare disinformazione: le risposte europee ai* deepfakes, in questa *Rivista*, 1, 2023, 170 ss.

[65] La dottrina ha quindi evidenziato come il DSA, in tal senso, adotti un approccio in qualche misura

La scelta finale e "di merito" circa le *policy* da adottare in concreto, quindi, spetterà sempre agli operatori, il che ci pare sia un tema molto significativo anche sul versante sanzionatorio, nella misura in cui il DSA, in tale ambito, potrà a rigore dirsi violato allorquando i soggetti regolati abbiamo in tutto o in parte omesso o non effettuato correttamente[66], secondo i predetti generali criteri metodologici di analisi e gestione, lo svolgimento delle attività di *risk assessment* e *management*, e non già, di per sé, per la (motivata) scelta di non adottare (o di adottare in un certo modo) le specifiche, singole misure di gestione del rischio, rispetto alla quale le *corporation* mantengono un autonomo potere decisorio; nell'introdurre l'elenco delle tipologie di politiche di mitigazione dei rischi suggerite alle piattaforme, invero, il testo originale in inglese del DSA utilizza la chiara dicitura per cui «such measures *may*[67] include» (cioè possono, non devono).
Ai sensi dei parr. 2 e 3 dell'art. 35, ad ogni modo, le istituzioni europee potranno adottare periodicamente relazioni e orientamenti volti ad agevolare, secondo dinamiche flessibili e tali da assicurare anche consultazioni pubbliche con un coinvolgimento preventivo dei vari *stakeholder*, la diffusione delle *best practice* implementate nel settore e informazioni di rilievo circa i rischi sistemici più rilevanti, così da aiutare concretamente le piattaforme online e i motori di ricerca ad adeguarsi a tali obblighi di *compliance*, fornendo loro indicazioni ancor più puntuali sulle migliori strategie da attuare per conseguire gli obiettivi di prevenzione fissati dal regolamento[68].

riportabile al concetto di *meta-regulation* o *enforced-self regulation*: v. N. Zingales, *The DSA as a Paradigm Shift for Online Intermediaries' Due Diligence*, in J. van Hoboke - J.P. Quintais - N. Appelman - R. Fahy - I. Buri - M. Straub (a cura di), *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implications*, Berlino, 2023, 213-214, il quale, da un lato, evidenzia che «*This approach, which on the one hand leaves businesses with a significant amount of discretion in the implementation of regulatory principles, and on the other involves a process of continuous evaluation and monitoring of the results, has been called "metaregulation" or "enforced self-regulation": "meta" because one (macro) regulator oversees another (micro) regulator in their management of risk; "enforced" because, in case of inadequacy of the self-regulatory practices, the (macro) regulator has the power to take enforcement measures», e, dall'altro lato, che «while the shift to a metaregulatory model should be welcomed for enabling reflexive and adaptive regulation, we must also be weary of its risk of collapsing in the absence of well-resourced and independent institutions*». Per un inquadramento approfondito del fenomeno dell'autonormazione (e delle varie classificazioni operabili) in relazione al sistema penale v. la recente indagine monografica di D. Bianchi, *Autonormazione e diritto penale. Intersezioni, potenzialità, criticità*, Torino, 2022.

66 Ad esempio, effettuando soltanto un'analisi molto vaga, sommaria e superficiale dei rischi legati, in generale, a un certo *business* digitale, senza tarare tale *assessment* sulle proprie specificità, sulle proprie concrete dinamiche operative, sui propri servizi, nella logica di una valutazione realmente *tailor made*.

67 Corsivo nostro.

68 In particolare, si prevede che «2. Il comitato, in cooperazione con la Commissione, pubblica relazioni annuali esaustive. Le relazioni comprendono gli elementi seguenti: a) individuazione e valutazione dei rischi sistemici più rilevanti e ricorrenti segnalati dai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi o identificati mediante altre fonti di informazione, in particolare le informazioni fornite in conformità degli articoli 39, 40 e 42; b) le migliori pratiche che consentano ai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi di attenuare i rischi sistemici individuati. Tali relazioni presentano i rischi sistemici suddivisi per Stato membro in cui si sono verificati e in tutta l'Unione, se del caso. 3. La Commissione, in cooperazione con i coordinatori dei servizi digitali, può emanare orientamenti sull'applicazione del paragrafo 1 in relazione a rischi concreti, con l'obiettivo specifico di presentare le migliori pratiche e raccomandare eventuali misure, tenendo debitamente conto delle possibili conseguenze di tali misure sui diritti fondamentali di tutte le parti interessate sanciti dalla Carta. Nell'elaborazione di tali orientamenti la Commissione organizza consultazioni pubbliche». Inoltre, ai sensi dell'art. 44 del DSA «1. La Commissione consulta il comitato e sostiene e promuove lo sviluppo e l'attuazione di norme volontarie fissate dai competenti organismi di normazione europei e internazionali

L'auspicio, dunque, è che tale interazione tra disciplina normativa e orientamenti integrativi fornite dalle autorità di *enforcement*, che sembra in qualche misura ispirarsi a pratiche ampiamente sperimentate in molti ordinamenti specie con riferimento alla *corporate criminal liability*[69], possa delineare chiaramente le regole del gioco, alla luce del non facile compito qui assegnato dal DSA alle organizzazioni più importanti del mondo digitale. Specie nel settore del contrasto alla disinformazione, del resto, la costruzione e l'implementazione di *policy* da parte delle piattaforme presuppone una complessa opera di bilanciamento tra diritti fondamentali individuali e collettivi tra loro contrapposti, per cui occorre che quella alle *Big Tech* private non sia una delega totalmente "in bianco", ma, al contrario, sia frutto di una strategia di gestione condivisa di tali rischi[70], sotto la guida dei decisori pubblici, anche e soprattutto alla luce dei rilevanti poteri sanzionatori che possono essere azionati in caso di omesso o non corretto adeguamento a tali obblighi di *due diligence* da parte di questi soggetti economici.

4.3. Il *crisis response mechanism*

L'art. 36 del DSA disciplina una procedura particolare destinata ad applicarsi, con riferimento a piattaforme online e motori di ricerca di dimensioni molto grandi, in condizioni di crisi definite espressamente come «circostanze eccezionali [che] comportano una grave minaccia per la sicurezza pubblica o la salute pubblica nell'Unione o in parti significative di essa». Il considerando 91 del regolamento fornisce, peraltro, alcuni esempi significativi, specificando che tali «crisi potrebbero derivare da conflitti armati

almeno per quanto riguarda: a) la presentazione elettronica delle segnalazioni di cui all'articolo 16; b) modelli, progettazione e norme di processo per comunicare con i destinatari del servizio in modo facilmente fruibile sulle restrizioni derivanti dalle condizioni generali e sulle relative modifiche; c) la presentazione elettronica di segnalazioni da parte dei segnalatori attendibili a norma dell'articolo 22, anche per mezzo di interfacce di programmazione delle applicazioni; d) interfacce specifiche, comprese le interfacce di programmazione delle applicazioni, per agevolare il rispetto degli obblighi di cui agli articoli 39 e 40; e) le revisioni delle piattaforme online di dimensioni molto grandi e dei motori di ricerca online di dimensioni molto grandi a norma dell'articolo 37; f) l'interoperabilità dei registri della pubblicità di cui all'articolo 39, paragrafo 2; g) la trasmissione di dati tra intermediari pubblicitari a sostegno degli obblighi di trasparenza a norma dell'articolo 26, paragrafo 1, lettere b), c) e d); h) misure tecniche che consentano il rispetto degli obblighi in materia di pubblicità di cui al presente regolamento, compresi gli obblighi riguardanti i contrassegni ben visibili per la pubblicità e le comunicazioni commerciali di cui all'articolo 26; i) interfacce di scelta e presentazione delle informazioni sui principali parametri dei diversi tipi di sistemi di raccomandazione, conformemente agli articoli 27 e 38; j) norme per misure mirate a tutela dei minori online. 2. La Commissione sostiene l'aggiornamento delle norme alla luce degli sviluppi tecnologici e del comportamento dei destinatari dei servizi in questione. Le informazioni pertinenti relative all'aggiornamento delle norme devono essere disponibili al pubblico e facilmente accessibili».

[69] V. da ultimo l'approfondita indagine monografica di R. Sabia, *Responsabilità da reato degli enti e paradigmi di validazione dei modelli organizzativi. Esperienze comparate e scenari di riforma*, Torino, 2022.

[70] V. l'introduzione alla presente ricerca di A. Gullo, *Contenuti, scopi e traiettoria della ricerca: le nuove frontiere della* compliance *nel mercato digitale*. Su tali profili, in relazione al DSA e con interessanti riferimenti alle indicazioni della giurisprudenza del Corte suprema federale tedesca, v. A. von Ungern-Sternberg, *Freedom of Speech goes Europe – EU Laws for Online Communication*, in A. von Ungern-Sternberg (a cura di), *Content Regulation in the European Union*, cit., 45; nello stesso volume cfr. anche il contributo di R. Janal, *Impacts of the Digital Services Act on the Facebook "Hate Speech" Decision by the German Federal Court of Justice*, 119 ss.

o atti di terrorismo, compresi conflitti o atti di terrorismo emergenti, catastrofi naturali quali terremoti e uragani, nonché pandemie e altre gravi minacce per la salute pubblica a carattere transfrontaliero».

Si tratta, a ben vedere, di ambiti particolarmente sensibili proprio rispetto al contrasto alle campagne (coordinate e non) di disinformazione; in numerosissimi casi, infatti, le notizie false maggiormente virali circolate in rete, e tali da poter influire negativamente sui diritti collettivi e individuali in gioco (salute e sicurezza pubblica), hanno avuto ad oggetto proprio le crisi internazionali in questione[71]. Appare quindi chiaro, e di interesse per questa ricerca, il retroterra "socio-criminologico" di riferimento di tale previsione.

Ora, in queste situazioni, la disposizione in questione del DSA prevede che la Commissione europea, su raccomandazione del comitato europeo per i servizi digitali[72], possa adottare una decisione «che impone» a tali operatori di intraprendere una o più tra le seguenti azioni: *a)* una valutazione sull'eventualità e, in caso affermativo, sulla portata e sul modo in cui il funzionamento o l'uso dei propri servizi può, si legge letteralmente, «contribuire» a una delle suindicate minacce gravi per la sicurezza o la salute pubblica; *b)* l'individuazione e l'applicazione di una delle misure di attenuazione dei rischi sistemici pocanzi menzionate e definite dall'art. 35, o dall'art. 48, par. 2, del DSA – si tratta, in quest'ultimo caso, dei protocolli di crisi volontari che possono essere elaborati, sperimentati e applicati, sempre per far fronte a analoghe situazioni emergenziali, tra tali organizzazioni e la Commissione europea[73] –, così da «prevenire, eliminare o limitare

[71] Si veda da ultimo il caso studio – in corso di pubblicazione sul sito istituzionale del MAECI – del terzo ciclo della presente ricerca (*Narrazioni e strategie di propaganda nelle* community *filorusse*), dedicato proprio alla disamina dei fenomeni di disinformazione legati al recente conflitto armato in Ucraina, cui si rinvia per ogni riferimento. In argomento v. anche L. Ciliberti, Free flow of information – *Il contrasto alla disinformazione in tempi di guerra*, in questa *Rivista*, 2, 2022, 349 ss., e S. Lattanzi, *La lotta alla disinformazione nei rapporti tra Unione e Stati terzi alla luce del conflitto russo-ucraino*, ivi, 3, 2022, 158 ss.

[72] L'art. 61 del DSA stabilisce invero che «1. È istituito un gruppo consultivo indipendente di coordinatori dei servizi digitali per la vigilanza sui prestatori di servizi intermediari denominato «comitato europeo per i servizi digitali» («comitato»). 2. Il comitato fornisce consulenza ai coordinatori dei servizi digitali e alla Commissione conformemente al presente regolamento per conseguire gli obiettivi seguenti: a) contribuire all'applicazione coerente del presente regolamento e alla cooperazione efficace dei coordinatori dei servizi digitali e della Commissione nelle materie disciplinate dal presente regolamento; b) coordinare e contribuire agli orientamenti e all'analisi della Commissione, dei coordinatori dei servizi digitali e di altre autorità competenti sulle questioni emergenti nel mercato interno in relazione alle materie disciplinate dal presente regolamento; c) assistere i coordinatori dei servizi digitali e la Commissione nella vigilanza sulle piattaforme online di dimensioni molto grandi».

[73] L'art. 48 nel dettaglio dispone che «1. Il comitato può raccomandare alla Commissione di avviare l'elaborazione, conformemente ai paragrafi 2, 3 e 4, di protocolli di crisi volontari per affrontare situazioni di crisi. Dette situazioni sono strettamente limitate a circostanze straordinarie che incidono sulla sicurezza pubblica o sulla salute pubblica. 2. La Commissione incoraggia e facilita i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi e, ove opportuno, i fornitori di altre piattaforme online o di altri motori di ricerca online a partecipare all'elaborazione, alla sperimentazione e all'applicazione di tali protocolli di crisi. La Commissione provvede affinché tali protocolli di crisi comprendano una o più delle misure seguenti: a) la ben evidenziata visualizzazione di informazioni sulla situazione di crisi fornite dalle autorità degli Stati membri o a livello di Unione o, a seconda del contesto della crisi, da altri organismi competenti affidabili; b) la garanzia che il fornitore di servizi intermediari designi uno specifico punto di contatto per la gestione delle crisi; ove opportuno, può trattarsi del punto di contatto elettronico di cui all'articolo 11 oppure, nel caso dei fornitori di piattaforme online di dimensioni molto grandi o di motori di ricerca online di

tale contributo alla grave minaccia individuata»; *c)* una relazione alla Commissione in merito alle misure adottate e alle valutazioni effettuate nel corso dell'implementazione di tale meccanismo di risposta alla crisi[74].

Ai sensi del par. 3, occorre che le azioni richieste dalla Commissione siano «strettamente necessarie, giustificate e proporzionate» tenuto conto della gravità della minaccia in corso e delle implicazioni, specie per i diritti fondamentali di tutte le parti interessate, delle misure richieste; la Commissione dovrà inoltre indicare «un termine ragionevole entro il quale devono essere adottate le misure specifiche» in questione, anche considerandone l'urgenza e il tempo necessario per la loro preparazione e attuazione; è stabilito in ogni caso che le azioni richieste debbano essere «limitate a un periodo non superiore a tre mesi», eventualmente prorogabili dalla Commissione per un periodo non superiore a ulteriori tre mesi[75]. L'organo di *enforcement* europeo, poi, dovrà mo-

dimensioni molto grandi, del responsabile della conformità di cui all'articolo 41; c) ove opportuno, l'adeguamento delle risorse destinate a garantire il rispetto degli obblighi di cui agli articoli 16, 20, 22, 23 e 35 alle esigenze che sorgono dalla situazione di crisi. 3. La Commissione coinvolge, se opportuno, le autorità degli Stati membri e può coinvolgere anche le istituzioni, gli organi e gli organismi dell'Unione nell'elaborazione, nella sperimentazione e nella supervisione dell'applicazione dei protocolli di crisi. Ove necessario e opportuno, la Commissione può coinvolgere anche le organizzazioni della società civile o altre organizzazioni competenti nell'elaborazione dei protocolli di crisi. 4. La Commissione mira a garantire che i protocolli di crisi definiscano chiaramente tutti gli elementi seguenti: a) i parametri specifici per determinare che cosa costituisca la specifica circostanza eccezionale che il protocollo di crisi intende affrontare e gli obiettivi che persegue; b) il ruolo dei singoli partecipanti e le misure che devono mettere in atto durante la fase preparatoria e in seguito all'attivazione del protocollo di crisi; c) una procedura chiara per stabilire quando debba essere attivato il protocollo di crisi; d) una procedura chiara per determinare il periodo durante il quale devono essere messe in atto le misure da adottare dopo l'attivazione del protocollo di crisi, periodo strettamente limitato a quanto necessario per far fronte alle specifiche circostanze eccezionali in questione; e) le garanzie necessarie per far fronte ad eventuali effetti negativi sull'esercizio dei diritti fondamentali sanciti dalla Carta, in particolare la libertà di espressione e di informazione e il diritto alla non discriminazione; f) una procedura per riferire pubblicamente in merito a tutte le misure adottate, alla loro durata e ai loro esiti, al termine della situazione di crisi. 5. Se ritiene che un protocollo di crisi non affronti efficacemente la situazione di crisi o non garantisca l'esercizio dei diritti fondamentali di cui al paragrafo 4, lettera e), la Commissione chiede ai partecipanti di rivedere tale protocollo, anche adottando misure supplementari». In argomento si veda anche la disamina effettuata nel capitolo 1 del presente report.

[74] In dettaglio, la lett. c) del par. 1 dell'art. 36 del DSA si riferisce alla predisposizione di «una relazione alla Commissione, entro una certa data o a intervalli regolari specificati nella decisione, in merito alle valutazioni di cui alla lettera a), sul contenuto preciso, l'attuazione e l'impatto qualitativo e quantitativo delle misure specifiche adottate a norma della lettera b) e su qualsiasi altra questione connessa a tali valutazioni o misure, come specificato nella decisione».

[75] Il par. 4 dell'art. 36 prevede altresì che «4. A seguito dell'adozione della decisione di cui al paragrafo 1, la Commissione adotta, senza indebito ritardo, tutte le seguenti misure: a) notifica la decisione al fornitore o ai fornitori destinatari della decisione; b) rende la decisione disponibile al pubblico; e c) informa il comitato della decisione, lo invita a presentare il proprio parere e lo tiene informato di eventuali sviluppi successivi relativi alla decisione». In base ai parr. 7, 10 e 11 della medesima previsione, poi, «7. La Commissione monitora l'applicazione delle misure specifiche adottate a norma della decisione di cui al paragrafo 1 del presente articolo sulla base delle relazioni di cui alla lettera c) di tale paragrafo e di ogni altra informazione pertinente, comprese le informazioni che può richiedere a norma dell'articolo 40 o 67, tenendo conto dell'evoluzione della crisi. La Commissione riferisce periodicamente al Comitato in merito a tale monitoraggio, almeno una volta al mese. […] 10. La Commissione tiene nella massima considerazione le raccomandazioni del comitato a norma del presente articolo. 11. La Commissione riferisce al Parlamento europeo e al Consiglio una volta all'anno a seguito dell'adozione di decisioni di cui al presente articolo e, in ogni caso, tre mesi dopo la fine della crisi, in merito all'applicazione delle misure specifiche adottate a norma di tali decisioni».

nitorare l'applicazione da parte dell'operatore delle misure in parola, avviando se del caso un "dialogo" con quest'ultimo per valutare l'efficacia di tali azioni e richiedendo eventualmente al soggetto regolato di riesaminarle, previa consultazione del Comitato, ferma restando la possibilità, in ogni caso, di revocare la decisione di applicare il meccanismo di risposta alla crisi tenendo conto dell'evoluzione (e specie della cessazione) della situazione emergenziale.

Emerge con chiarezza, tra le righe della disposizione, lo sforzo del legislatore eurounitario di bilanciare le esigenze contrapposte in gioco.

È evidente, invero, come vi sia la consapevolezza dell'attribuzione alla Commissione europea di poteri particolarmente significativi, che gli danno la possibilità di incidere significativamente, con un provvedimento "individuale" e di carattere certamente non poco invasivo, sull'esercizio delle attività di piattaforme online e motori di ricerca di dimensione molto grandi, imponendogli, in tempi molto stretti e con particolare urgenza, l'adozione di diverse misure che presuppongono ponderazioni difficili e scelte molto delicate e complesse alla luce del loro impatto sui diritti fondamentali, specie in simili situazioni d'emergenza. Non è del resto un caso che – tenuto conto delle possibili ripercussioni di tali procedure sia sui diritti delle *corporation* cui vengono richieste le azioni di risposta alla crisi, sia su quelli dei loro utenti che, "di rimbalzo", si troveranno a subire gli effetti dei provvedimenti emergenziali implementati dalle piattaforme e che possono risolversi in significative ingerenze sulla loro sfera giuridica – parte della dottrina abbia subito criticato la genericità e l'ampiezza dei presupposti in grado di innescare il potere della Commissione di applicare la disposizione in questione[76]. Si pensi, ad esempio, rispetto ai temi della presente ricerca e per meglio chiarire i termini problematici della questione, alla possibilità di applicare tale istituto per "reagire" a campagne di disinformazione su larga scala in occasione di conflitti armati internazionali o pandemie e altre crisi sanitarie gravi, con la richiesta alle piattaforme di modificare le loro condizioni generali d'uso del servizio, con l'effetto di impedire agli utenti di condividere determinate notizie circa lo scontro armato o la minaccia per la salute pubblica in corso; il rischio di forme di indebita censura e di compressione di fondamentali libertà democratiche è in queste ipotesi, evidentemente, tutt'altro che secondario.

Di qui, come forme di *counterbalance*, sia la decisione di perimetrare in un arco temporale molto circoscritto la possibilità di dar corso a tali meccanismi, sia l'importante indicazione di cui al par. 5 dell'art. 36, a tenore del quale la «scelta delle misure specifiche da adottare a norma del paragrafo 1, lettera b), e del paragrafo 7, secondo comma, spetta

[76] V. in particolare V. Colarocco - M. Cogode, *Gli obblighi applicabili a piattaforme* online *di dimensioni molto grandi (Artt. 33-43 – Capo III, Sezione 5)*, in *Diritto di internet*, 1, 2023, 32, ove si è osservato che «Le decisioni che riguardano la libertà di espressione e l'accesso alle informazioni, in particolare in tempi di crisi, non possono essere legittimamente prese dal solo potere esecutivo ma occorre un controllo parlamentare sull'esistenza e sulla durata della situazione emergenziale al fine di evitare abusi. La definizione di crisi deve, infatti, soddisfare i principi di chiarezza e specificità e non deve autorizzare la Commissione a mantenere misure di crisi per un periodo prolungato o indefinito. La definizione dovrebbe quindi, nella concreta interpretazione che ne verrà fornita, essere limitata alle minacce che sono in grado di destabilizzare seriamente le strutture costituzionali, politiche, economiche o sociali fondamentali dell'Unione o parti significative di esse. E il meccanismo proposto dovrebbe, a sua volta e per logica conseguenza, prevedere un ruolo più centrale degli organi rappresentativi dei cittadini, sottraendo all'esecutivo il potere unilaterale di limitare in modo quasi permanente l'accesso del pubblico alle informazioni e alla loro diffusione».

al fornitore o ai fornitori destinatari della decisione della Commissione»[77]. In linea con un approccio, come visto, che costituisce la cifra dell'intero regolamento, ci pare che tale locuzione debba essere interpretata nel senso che la Commissione possa imporre, nella propria decisione, soltanto l'adozione di un certo e ampio *genus* di misure (ad es., l'adeguamento dei sistemi di raccomandazione delle notizie, oppure delle condizioni generali o delle procedure di moderazione dei contenuti), dovendo essere lasciate al libero apprezzamento del soggetto regolato, in ultima istanza, la costruzione e l'attuazione specifica della *policy*, della misura di dettaglio da adottare, la scelta su "come mettere a terra" concretamente le modifiche delle proprie regole autonormate, senza che i poteri di ingerenza dell'organo pubblico europeo possano spingersi fino a obbligare gli attori privati ad adottare misure "predeterminate", escludendo qualsiasi margine di scelta su come implementare e integrare il tipo di provvedimenti richiesti all'interno del proprio contesto operativo interno.

4.4. L'*independent audit*

L'art. 37 del DSA, facendo propria una tipica metodologia della *corporate compliance*, sancisce l'obbligo per le piattaforme online e i motori di ricerca di dimensioni molto grandi di sottoporsi, a proprie spese «e almeno una volta all'anno», a *independent audit*[78] – effettuati da organizzazioni che soddisfino requisiti di indipendenza, comprovata esperienza, obiettività e deontologia professionale dettagliatamente normati dal par. 3 della disposizione[79] – volti a valutare la conformità dell'organizzazione: «a) agli obbli-

[77] Il par. 1 della stessa disposizione prevede altresì che «Nell'individuare e applicare le misure di cui alla lettera b) del presente paragrafo, il prestatore o i prestatori di servizi tengono debitamente conto della criticità della grave minaccia di cui al paragrafo 2, dell'urgenza delle misure e delle implicazioni effettive o potenziali per i diritti e gli interessi legittimi di tutte le parti interessate, compresa l'eventuale inosservanza dei diritti fondamentali sanciti dalla Carta».

[78] La previsione fornisce naturalmente ulteriori dettagli sia rispetto agli obblighi di cooperazione delle piattaforme nello svolgimento delle revisioni, sia con riferimento alla trasparenza e agli aspetti di riservatezza e segreto professionale correlati a tali attività, stabilendo in particolare al par. 2 che «I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi consentono alle organizzazioni che effettuano le revisioni a norma del presente articolo la cooperazione e l'assistenza necessarie per consentire loro di svolgere tali revisioni in modo efficace, efficiente e tempestivo, anche provvedendo a dare loro accesso a tutti i dati e ai locali pertinenti, e rispondendo a domande orali o scritte. Essi si astengono dall'ostacolare, influenzare indebitamente o compromettere lo svolgimento della revisione. Dette revisioni garantiscono un adeguato livello di riservatezza e il segreto professionale per quanto riguarda le informazioni ottenute dai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi e da terzi nel contesto delle revisioni, anche dopo la loro conclusione. Tuttavia, il rispetto di tale obbligo non deve pregiudicare l'esecuzione delle revisioni e delle altre disposizioni del presente regolamento, in particolare quelle in materia di trasparenza, vigilanza ed esecuzione. Se necessario ai fini della relazione sulla trasparenza a norma dell'articolo 42, paragrafo 4, la relazione di revisione e la relazione di esecuzione della revisione di cui ai paragrafi 4 e 6 del presente articolo sono accompagnate dalle versioni prive di informazioni che potrebbero essere ragionevolmente considerate riservate».

[79] Ove è stabilito che «Le revisioni effettuate a norma del paragrafo 1 sono eseguite da organizzazioni: a) indipendenti e in assenza di conflitti di interessi con il fornitore di piattaforme online di dimensioni molto grandi o di motori di ricerca online di dimensioni molto grandi in questione, e con qualsiasi persona giuridica connessa con tale fornitore; in particolare: i) non devono aver fornito servizi diversi dalla revisione relativi alle questioni sottoposte a revisione al fornitore della piattaforma online di

ghi stabiliti al capo III; b) agli impegni assunti a norma dei codici di condotta di cui agli articoli 45 e 46 e dei protocolli di crisi di cui all'articolo 48».

Al termine dell'attività di revisione, tali organismi redigeranno una relazione finale, che conterrà un giudizio circa il rispetto, da parte del soggetto regolato, dei detti obblighi stabiliti dal regolamento.

L'esito finale di tale revisione, in particolare, potrà essere «positivo», «positivo con osservazioni», o «negativo», in questi ultimi due casi dovendosi naturalmente fornire «raccomandazioni operative su misure specifiche per conseguire la conformità e sui tempi raccomandati per conseguirla»[80], con l'obbligo per le organizzazioni in questione di tener «debitamente conto» di queste ultime e di adottare, entro «un mese dal ricevimento di tali raccomandazioni» una «relazione di attuazione della revisione con cui stabiliscono tali misure» oppure forniscono adeguata giustificazione delle ragioni per cui ritengono di non darvi corso, descrivendo, tuttavia, le «misure alternative» adottate per risolvere tutte le "*instances of non-compliance*" che siano state identificate[81]. Quest'ultima specificazione, in particolare, costituisce l'ennesima conferma della scelta del legislatore eurounitario di non imporre mai l'adozione di specifiche *policy* di dettaglio, lasciando sempre alle piattaforme la decisione definitiva sulle modalità concrete di adempimento

dimensioni molto grandi interessata o del motore di ricerca online di dimensioni molto grandi in questione e a qualsiasi persona giuridica collegata a tale fornitore nei 12 mesi precedenti l'inizio della revisione, e devono essersi impegnati a non fornire tali servizi nei 12 mesi successivi al completamento della revisione; ii) non devono aver fornito servizi di revisione a norma del presente articolo al fornitore della piattaforma online di dimensioni molto grandi interessata o del motore di ricerca online di dimensioni molto grandi in questione e a qualsiasi persona giuridica collegata a tale fornitore per un periodo superiore a dieci anni consecutivi; iii) non possono effettuare la revisione a fronte di corrispettivi che dipendono dall'esito dello stesso; b) sono dotate di comprovata esperienza nel settore della gestione dei rischi, di competenze e di capacità tecniche; c) sono dotate di comprovata obiettività e deontologia professionale, basata in particolare sull'adesione a codici di condotta o standard appropriati».

[80] In dettaglio i parr. 4 e 5 dell'art. 37 del DSA prevedono che «4. I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi provvedono affinché le organizzazioni che effettuano le revisioni redigano una relazione per ciascuna revisione. Tale relazione è motivata per iscritto e contiene almeno gli elementi seguenti: a) il nome, l'indirizzo e il punto di contatto del fornitore della piattaforma online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi oggetto della revisione e il periodo di riferimento della revisione; b) il nome e l'indirizzo dell'organizzazione o delle organizzazioni che eseguono la revisione; c) una dichiarazione di interessi; d) una descrizione degli elementi specifici sottoposti a revisione e della metodologia applicata; e) una descrizione e una sintesi delle principali constatazioni derivanti dalla revisione; f) un elenco delle parti terze consultate nel quadro della revisione; g) un giudizio di revisione sul rispetto, da parte del fornitore della piattaforma online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi oggetto della revisione, degli obblighi e degli impegni di cui al paragrafo 1, giudizio che può essere segnatamente «positivo», «positivo con osservazioni» o «negativo»; h) se il giudizio di revisione non è «positivo», raccomandazioni operative su misure specifiche per conseguire la conformità e sui tempi raccomandati per conseguirla. 5. Qualora l'organizzazione che ha effettuato la revisione non abbia potuto verificare determinati elementi specifici o esprimere un giudizio di revisione sulla base delle proprie indagini, la relazione di revisione include una spiegazione delle circostanze e dei motivi per cui tali elementi non hanno potuto essere sottoposti a revisione».

[81] Ai sensi del par. 7 dell'art. 37 del DSA, peraltro, e in linea con altre analoghe previsioni del regolamento, viene conferito alla Commissione europea «il potere di adottare atti delegati conformemente all'articolo 87 al fine di integrare il presente regolamento stabilendo le norme necessarie per lo svolgimento delle revisioni a norma del presente articolo, in particolare per quanto riguarda la regolamentazione necessaria per le fasi procedurali, le metodologie di revisione e i modelli di comunicazione delle revisioni effettuate a norma del presente articolo. Tali atti delegati tengono conto di eventuali standard di revisione volontari a norma dell'articolo 44, paragrafo 1, lettera e)».

ai doveri di *due diligence* loro imposti.
Si tratta, in definitiva, di una disposizione "di chiusura" che, unitamente all'art. 41 del DSA relativo all'istituzione di una specifica *compliance function* aziendale, sul quale subito ci soffermeremo[82], completa il novero degli obblighi gravanti sui grandi *player* del mercato digitale, chiamati a confrontarsi con organismi indipendenti esterni in merito alla correttezza del proprio apparato rispetto a quanto richiesto dal nuovo regolamento europeo. È un ulteriore *step* di una strategia di regolazione volta a garantire il più possibile l'effettività e la correttezza del *private enforcement* di operatori il cui impegno proattivo sarà essenziale per consentire il raggiungimento degli obiettivi della riforma[83].

4.5. L'istituzione di una specifica funzione aziendale di *compliance* per monitorare la conformità dell'organizzazione agli obblighi del DSA

L'art. 41 del DSA, come anticipato, "chiude" il cerchio degli obblighi aggiuntivi gravanti sulle piattaforme online e sui motori di ricerca di dimensioni molto grandi, stabilendo che questi ultimi debbano istituire una specifica *compliance function* al fine di monitorare la conformità dell'organizzazione agli obblighi sanciti dal nuovo regolamento; dovrà trattarsi di una articolazione societaria indipendente dalle funzioni operative, composta da uno o più "*compliance officer*s", compreso l'*head* di tale "ufficio" (quale figura che in qualche modo si 'ispira' a quella del DPO in ambito *privacy*).
La previsione in questione, in linea con le consolidate *best practice* in tema di *corporate governance*, delinea una funzione di controllo a diretto riporto dell'organo di gestione, composta, quanto all'*head*, da un «un alto dirigente indipendente con responsabilità distinta per la funzione di controllo della conformità», nonché, quanto ad ogni altro componente, da soggetti in possesso delle «qualifiche professionali, delle conoscenze, dell'esperienza e delle capacità necessarie».
L'organo di gestione manterrà la responsabilità ultima in ordine alla approvazione e al riesame periodico delle strategie di valutazione, gestione e monitoraggio dei rischi (in particolare quelli di cui all'art. 34 del DSA), nonché rispetto alla costruzione di sistemi di *governance* che garantiscano, anche tramite la separazione delle responsabilità e la prevenzione dei conflitti di interesse, l'indipendenza della funzione di DSA *compliance* e l'assegnazione ai relativi *officer* di risorse, *status* e poteri necessari per adempiere alle proprie funzioni[84].
I compiti di tale funzione di *compliance* consistono, appunto, nel vigilare sul rispetto da

[82] Cfr. il paragrafo successivo.

[83] In dottrina, ad ogni modo, non si è mancato di identificare alcuni possibili rischi, nella misura in cui «*VLOPs may leverage their market power against their new mandatory auditors and risk assessors, a threat theorised as 'audit capture'*»: cfr. J. Laux - S. Wachter - B. Mittelstadt, *Taming the few: Platform regulation, independent audits, and the risks of capture created by the DMA and DSA*, in *Computer Law & Security Review*, 1, 2021, 43.

[84] Si prevede, inoltre, che l'*head* della funzione di *compliance* non possa essere rimosso senza previa approvazione dell'organo di gestione e l'obbligo per i soggetti di regolati di comunicare nominativo e riferimenti di tale soggetto al coordinatore dei servizi digitali del luogo di stabilimento e alla Commissione europea.

parte della *corporation* delle *obligation* sancite dal DSA. In particolare, tale organismo sarà chiamato a: collaborare con il coordinatore dei servizi digitali del luogo di stabilimento e con la Commissione; assicurare il corretto svolgimento delle attività di *risk assessment* e *management* di cui agli artt. 34 e 35 del DSA; organizzare e sovraintendere agli adempimenti connessi agli *independent audit* di cui all'art. 37; informare e consigliare i dirigenti e i dipendenti dell'organizzazione in merito agli obblighi del regolamento ed esercitare un ruolo di impulso nei confronti dell'organo di gestione rispetto a tutte le questioni connesse alla DSA *compliance*; monitorare la conformità agli obblighi connessi ai codici di condotta e ai protocolli di crisi *ex* artt. 45 e ss. del DSA.

A fronte dell'inesistenza di un *dovere generale* per le società di istituire una simile funzione societaria, come noto resa obbligatoria esclusivamente in specifici ambiti settoriali[85], è quindi molto significativo notare come il legislatore europeo abbia scelto qui di rendere cogente la sua costituzione, con una decisione che è del resto in linea, come detto, con le *policy* fatte proprie da fonti normative analoghe; la presenza di un punto di riferimento unico all'interno dell'organizzazione, che sovraintenda alle varie attività di controllo della conformità, e svolga un ruolo di impulso e di coordinamento complessivo dei correlati adempimenti, facendo da "collettore" delle varie istanze, è invero giustamente considerata un passaggio essenziale di completamento della disciplina, a presidio della sua efficacia.

Sarà, per il resto, importante verificare come la prassi si orienterà rispetto all'organizzazione e al funzionamento concreto della funzione di DSA *compliance*.

Due ci sembrano gli aspetti più rilevanti.

Anzitutto, la lettera del regolamento consente espressamente di scegliere tra una composizione monocratica o collegiale. Se da un lato una maggiore flessibilità può sembrare apprezzabile, di contro è molto difficile ipotizzare che, nel contesto di *corporation* di "dimensioni molto grandi", un unico funzionario possa assicurare uno svolgimento realmente efficace dei compiti assegnati a tale articolazione in organizzazioni complesse con una considerevole mole di utenti e, quindi, di *workflow*. Ci sembra sia preferibile allora, quantomeno di regola, optare per la nomina di plurimi responsabili, in numero adeguato alle specificità di ogni operatore.

In secondo luogo, in base la lettera del regolamento non è chiaro se debba trattarsi di un organismo da istituire totalmente *ex novo*, o se le responsabilità definite dall'art. 41 DSA possano essere assegnate a o uno o più componenti delle funzioni di *compliance* eventualmente già esistenti nelle organizzazioni (come è molto probabile che sia in enti di questo tipo), sempre, naturalmente, a condizione che tali uffici e i loro singoli membri – che la piattaforma voglia designare come DSA *compliance officer* – soddisfino i predetti requisiti delineati dal nuovo regolamento europeo. Il testo originale, che utilizza la locuzione «*shall establish*» ("istituiscono" nella traduzione italiana), non pare offrire certezze in merito, pur sembrando maggiormente "evocare"[86], almeno a livello strettamente letterale, la creazione di una nuova struttura. Tuttavia, a noi pare sia ragio-

[85] Cfr. chiaramente, ad esempio, l'art. 7 del Codice di autodisciplina delle società quotate italiane, reperibile in *borsaitaliana.it*.

[86] A conclusioni diverse si sarebbe senza alcun dubbio giunti nel caso di utilizzo di termini più neutri come "designare" o "nominare" ("*appoint*" in lingua inglese).

nevole (e conforme alla *ratio* del regolamento[87]) considerare legittima la seconda soluzione, se del caso costruendo un *team* "*ad hoc*" all'interno dell'ufficio già presente, anche per assicurare una ragionevole allocazione delle risorse organizzative e finanziarie e lo sfruttamento di quelle già esistenti, nell'ottica di una *compliance* realmente integrata quale approccio ormai indispensabile in uno scenario regolatorio sempre più complesso e variegato per i soggetti metaindividuali.

5. Riflessioni conclusive e indicazioni di *policy*

Il DSA è riuscito a colmare una significativa lacuna che caratterizzava lo scenario normativo europeo e di diversi Stati membri, in un panorama regolamentare in cui si erano iniziate ad affacciare, a "macchia di leopardo" e in singoli ordinamenti, iniziative legislative parziali[88], che toccavano solo alcuni punti dei profili poi organicamente ricondotti ad unità dalla nuova normativa eurounitaria; ciò anche con riferimento alla responsabilizzazione degli operatori digitali nelle attività di autonormazione e auto-organizzazione che abbiamo descritto in questa parte della ricerca. Ed è peraltro molto importante che ci si sia fatti carico di risolvere tale *gap* mediante un regolamento europeo, trattandosi di uno strumento per definizione più adatto a disciplinare un fenomeno, afferente ai più importanti modelli di *business* digitali, per sua natura transnazionale e che necessita, inevitabilmente, di risposte di pari respiro e non già esclusivamente "locali".

Anche solo guardando alla situazione immediatamente precedente l'approvazione del DSA, quindi, si può essere soddisfatti dei risultati raggiunti. La sensazione è quella di essere di fronte a un prodotto normativo di buona fattura, pure al netto di alcune criticità che abbiamo cercato di porre in evidenza e che forse, in fin dei conti, sono del tutto comprensibili in un atto legislativo che è stato giustamente ed efficacemente definito come "pioneristico"[89]. Insomma, si tratta di un percorso in cui, nel complesso, le luci prevalgono sulle ombre.

Giunti alla fine di questo contributo, non resta allora che tentare di fornire alcune indicazioni di *policy* che confluiranno nel documento contenuto in calce allo studio in cui, come per gli scorsi cicli della ricerca, avremo cura di tesaurizzare i risultati delle indagini condotte nelle varie sezioni in cui è stata articolata la nostra disamina del DSA, costruendo un prospetto unitario di raccomandazioni rivolte ai vari attori del settore.

Procediamo con ordine, ripercorrendo nella stessa "direzione di marcia" fin qui seguita i vari temi di cui ci siamo occupati in questo lavoro e cercando di isolare le questioni

[87] Del resto, ciò in qualche modo potrebbe contribuire anche a chiarire la ragione per cui il DSA consente di nominare anche un solo responsabile della conformità.

[88] Cfr. *supra* par. 1. Per un'analisi che ha messo in evidenza tale evoluzione del panorama normativo europeo, anche con richiami ad alcuni «*worrying trends toward criminalisation*», v. R. Ò Fathaigh - N. Helberger - N. Appelman, *The perils of legally defining disinformation*, in *Internet Policy Review*, 10(4), 2021, 2 ss.

[89] V. l'introduzione alla presente ricerca di A. Gullo, *Contenuti, scopi e traiettoria della ricerca*, cit. Non a caso in dottrina si è rilevato come «*the DSA is likely to shape the global approach to content regulation in this emerging area of law*»: cfr. P. Church - C.N. Pehlivan, *The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability*, in *Global Privacy Law Review*, 4(1), 2023, 53 ss.

maggiormente importanti dall'angolo visuale del contrasto alla disinformazione.
Quattro sono gli aspetti su cui, a nostro avviso, occorre concentrare l'attenzione.
Un primo tema attiene alla definizione di termini e condizioni del servizio (c.d. standard della *community*). Qui, come visto[90], le piattaforme dovrebbero rafforzare l'apparato di garanzie minime definito dall'art. 14, disciplinando l'esercizio dei propri poteri "sanzionatori" nel rispetto di diritti essenziali che devono necessariamente essere riconosciuti nell'implementazione di qualsiasi paradigma punitivo, anche in ambito privato: la legalità delle violazioni e delle misure sanzionatorie/interdittive, con i corollari della irretroattività, della tassatività/precisione delle previsioni punitive e del divieto di analogia; la dettagliata definizione dei soggetti titolari della potestà di dettare tali regole; il principio di proporzionalità del trattamento sanzionatorio; il divieto di responsabilità oggettiva e l'affermazione del principio di colpevolezza, etc.
Per ciò che concerne nello specifico la strutturazione di *policy* anti-disinformazione può essere rischioso e controproducente limitarsi a prevedere un generale divieto per gli utenti, invero troppo ampio e indeterminato, di condivisione di notizie false. La difficoltà, come sappiamo[91], di segnare un preciso confine tra esternazioni di fatti e opinioni personali, oggettivo e soggettivo, vero e falso, finirebbe per rendere tale "regola interna" difficilmente attuabile dai soggetti chiamati, all'interno dell'organizzazione, a moderare i contenuti immessi in rete dagli utenti e, soprattutto, per risolversi in molti casi in una indebita compressione della libertà di espressione dei destinatari del servizio.
Nella strutturazione di *term and conditions*, da tale specifica prospettiva, occorre allora introdurre divieti ben circostanziati, circoscritti, tassativi, con un approccio *case by case* e procedendo per singoli settori sensibili, vietando, ad esempio, l'intenzionale condivisione di notizie obiettivamente qualificabili come non vere per cui si riportino inesistenti difficoltà di accesso ai seggi elettorali o nelle operazioni di voto, con l'obiettivo di disincentivare le persone a recarsi alle urne e ledendo quindi l'interesse all'integrità ai processi elettorali, o notizie di analogo tenore volte ad arrecare pregiudizio a campagne vaccinali a tutela della salute pubblica, e così via.
Ancora, non dovrebbero essere consentite, a prescindere dal contenuto della notizia condivisa (e dalla sua veridicità), specifiche modalità decettive di utilizzo del servizio come l'interazione artificiosa tra più *account* o l'uso di *bot* automatici al fine di aumentare fraudolentemente la visibilità di certe informazioni.
I settori sensibili nei quali disciplinare e applicare tali politiche interne di gestione del servizio, inoltre, andrebbero identificati tramite un'analisi dei rischi svolta secondo i criteri di cui all'art. 34 DSA, le cui indicazioni di metodo dovrebbero essere seguite anche da piattaforme e motori di ricerca non qualificati come organizzazioni di "dimensioni molto grandi", pur, naturalmente, tenendo conto delle proprie specificità operative e organizzative e adattando di conseguenza i detti principi di *assessment*. Bisognerà poi coordinare la costruzione di tali standard della *community* con le conseguenti

[90] Cfr. *supra* par. 1.1.

[91] Per una più ampia disamina, e altri riferimenti bibliografici, sia consentito rinviare ancora a E. Birritteri, *Punire la disinformazione*, cit., 304 ss.

misure di mitigazione del rischio anche sul versante tecnico[92], tra cui la riduzione della visibilità o la c.d. demonetizzazione dei contenuti, la revisione dei sistemi di raccomandazione e pubblicità per evitare che dette informazioni diventino virali, l'utilizzo di contrassegni ben visibili per consentire agli utenti di identificare chiaramente i c.d. *deep fake* (e per dare la possibilità agli autori di *post* che li immettano in rete di indicare chiaramente la loro natura "falsa"[93]), unitamente a ogni altro accorgimento, sul piano del funzionamento concreto del servizio, indispensabile per rendere tale *enforcement* realmente efficace.

Una seconda questione concerne i meccanismi di *notice and action*: abbiamo infatti rilevato[94] che rispetto al contrasto alla disinformazione diversi contenuti o modalità d'utilizzo del servizio non possono spesso dirsi di per sé illegali; di conseguenza, le piattaforme online dovrebbero rendere disponibili i propri sistemi interni di segnalazione anche per l'invio di report che evidenzino semplicemente l'incompatibilità del contenuto con i c.d. standard della *community* (e in particolare con le *policy* dettate in materia di condivisione di notizie false).

Un terzo punto cruciale riguarda i sistemi interni di gestione dei reclami, trattandosi di un profilo particolarmente delicato dell'*enforcement* privato delle politiche anti-disinformazione, alla luce della tensione che inevitabilmente si genera tra esse e il rispetto della libertà di espressione. Per tali ragioni, anche in tal caso a nostro avviso è necessario che le piattaforme assicurino un livello maggiore di garanzie rispetto a quello minimo richiesto dagli artt. 17 e 20 del DSA, assicurando agli utenti, tra l'altro, un pieno contraddittorio preventivo, la garanzia di sufficiente autonomia e indipendenza (con riferimento alla distribuzione dei poteri dell'organizzazione) dei soggetti deputati a irrogare la sanzione e a decidere sui connessi reclami, il diritto di richiedere il riesame della decisione già a livello interno[95].

Un ultimo aspetto, infine, è quello legato al rafforzamento degli strumenti di monitoraggio continuo dell'efficacia dell'apparato di DSA *compliance* realizzato da queste organizzazioni[96], essendo auspicabile che anche piattaforme e motori di ricerca non designati come operatori "di dimensioni molto grandi" nominino *compliance officer* dedicati e si sottopongano, ove possibile, ad *audit* interni ed esterni indipendenti su base volontaria, pur con un approccio improntato a un'ampia flessibilità e alla possibilità di modellare gli adempimenti alla luce delle proprie specificità. Considerata la natura estremamente sensibile di tali pratiche di autonormazione, e per certi versi anche

---

92 Per un inquadramento di queste misure, con particolare riferimento ai filtri tecnici, v. M. Steinebach, *Potential and Limits of Filter Technology for the Regulation of Hate Speech and Fake News*, in A. von Ungern-Sternberg (a cura di), *Content Regulation in the European Union*, cit., 13 ss.

93 L'art. 35, par. 1, lett. k), del DSA si riferisce, come abbiamo già evidenziato, al ricorso «a un contrassegno ben visibile per fare in modo che un elemento di un'informazione, sia esso un'immagine, un contenuto audio o video, generati o manipolati, che assomigli notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che a una persona appaia falsamente autentico o veritiero, sia distinguibile quando è presentato sulle loro interfacce online e, inoltre, la fornitura di una funzionalità di facile utilizzo che consenta ai destinatari del servizio di indicare tale informazione».

94 Cfr. *supra* par. 2.1.

95 V. anche *supra* par. 3.1.

96 Cfr. *supra* parr. 4.4 e 4.5.

l'indubbia difficoltà di implementare una strategia di contrasto alla disinformazione, infatti, appare essenziale non soltanto avvalersi di figure incaricate di monitorare la conformità dell'organizzazione agli obblighi del DSA, e la loro efficace attuazione, ma anche favorire un proficuo confronto tra la *corporation* e i vari attori del sistema, dal momento che solo una ampia e costante cooperazione tra i diversi *stakeholder* potrà realmente assicurare il raggiungimento degli obiettivi che questa ambiziosa riforma ha cercato di conseguire all'esito di un difficile bilanciamento di tutti gli interessi in gioco.

Contrasto alla disinformazione, *Digital Services Act* e attività di private *enforcement*: fondamento, contenuti e limiti degli obblighi di *compliance* e dei poteri di autonormazione degli operatori*

Emanuele Birritteri

Abstract

Il contributo esamina l'impatto del Digital Services Act sull'attività di private enforcement per la moderazione dei contenuti immessi in rete dagli utenti – con la correlata due diligence – svolta dagli operatori digitali. Vengono analizzati fondamento, contenuti e limiti degli obblighi di compliance e dei poteri di autonormazione attribuiti al riguardo ai vari attori del sistema, mettendone in evidenza punti di forza e criticità con particolare riferimento alle strategie di contrasto alla disinformazione in rete. La parte finale dello scritto delinea alcune indicazioni di policy rivolte ai soggetti che saranno chiamati a conformarsi alle previsioni del nuovo Regolamento europeo.

This article aims at analysing the impact of the Digital Services Act on private enforcement activities for the moderation of user content – with the related due diligence – carried out by digital operators. In particular, the contribution examines the basis, content and limits of compliance obligations and self-regulatory powers attributed to the various actors involved, highlighting strengths and weaknesses, with a focus on strategies for combating disinformation online. The final part of the paper outlines some policy recommendations for subjects that will be required to comply with the provisions of this new European regulation.

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

Sommario

Keywords

Digital Services Act – *Compliance* – Autonormazione – *Due diligence* – *Private enforcement*

1. L'impatto del DSA sulle attività di *private enforcement* per il contrasto alla disinformazione: inquadramento generale

Nel corso dei primi due cicli della sezione giuridica di questa ricerca abbiamo rilevato come l'implementazione di strategie di contrasto alla disinformazione in rete non possa che fare affidamento sul coinvolgimento proattivo delle piattaforme online e degli operatori del mercato digitale, nella consapevolezza, come abbiamo cercato di dimostrare, dell'impossibilità di utilizzare il diritto criminale per punire di per sé la diffusione di notizie false, fuori dai casi in cui ciò arrechi pregiudizio ad interessi diversi dalla mera veridicità dell'informazione e per cui si ritenga possibile e necessaria la tutela penale[1].

Abbiamo altresì messo in luce come i decisori pubblici e gli studiosi del diritto punitivo debbano oggi necessariamente occuparsi delle pratiche di *private enforcement* tipiche di tale settore, dato che le attività di moderazione dei contenuti immessi in rete dagli utenti, realizzate soprattutto dalle grandi *corporation* digitali, possono incidere in misura significativa sui diritti fondamentali degli utenti (su tutti, la libertà di espressione), nel contesto di grandi arene digitali che, pur gestite da organizzazioni private, rappre-

[1] Sia consentito, anche per una più ampia *literature review*, il rinvio a E. Birritteri, *Punire la disinformazione: il ruolo del diritto penale e delle misure di moderazione dei contenuti delle piattaforme tra pubblico e privato*, in *Diritto penale contemporaneo – Rivista Trimestrale*, 4, 2021, 304 ss.

sentano oggi uno spazio di dibattito pubblico di rilevante importanza[2]. Ciò, inevitabilmente, finisce per "consegnare" nelle mani di tali *Big Tech* un grande potere, avendo tali soggetti collettivi la possibilità di farsi arbitri di tali dinamiche di interazione sociale e di esercitare una potestà "sanzionatoria" – in termini di rimozione di contenuti, disabilitazione di *account* anche di rilevanti personaggi politici, etc. – che può innescare un pericoloso *chilling effect* avuto riguardo al libero confronto democratico[3].

Di qui la necessità di costruire una cornice di regolazione pubblica volta a fissare le regole del gioco in materia, nell'ambito della quale gli operatori possano svolgere tali attività di autonormazione e "sanzionatorie" secondo regole fissate dal legislatore e sotto il controllo delle autorità pubbliche[4].

Il nuovo regolamento (UE) 2022/2065 relativo al mercato unico dei servizi digitali (*Digital Services Act*, d'ora in poi DSA) del 19 ottobre 2022[5] cerca di rispondere esattamente a tale esigenza, da un lato, prendendosi atto che gli «Stati membri stanno sempre più introducendo o stanno valutando di introdurre legislazioni nazionali sulle materia disciplinate dal presente Regolamento, imponendo in particolare obblighi di diligenza per i prestatori di servizi intermediari per quanto riguarda il modo in cui dovrebbero contrastare i contenuti illegali, la *disinformazione online* e altri rischi per la società»[6] e che alla luce «del carattere intrinsecamente transfrontaliero di internet […] tali legislazioni nazionali divergenti incidono negativamente sul mercato interno, che […] comporta uno spazio senza frontiere interne»[7]; dall'altro lato, riconoscendosi che, appunto, «un comportamento responsabile e diligente da parte dei prestatori di servizi intermediari è essenziale per un ambiente online sicuro, prevedibile e affidabile e per consentire ai cittadini dell'Unione e ad altre persone di esercitare i loro diritti fondamentali garantiti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), in particolare la libertà di espressione e di informazione, la libertà di impresa, il diritto alla non discriminazione e il conseguimento di un elevato livello di protezione dei consumatori»[8].

Obiettivo di questa sezione della presente ricerca è quello di esaminare l'impatto del DSA sull'attività di *private enforcement* per la moderazione dei contenuti immessi in rete dagli utenti – con la correlata *due diligence* – svolta dagli operatori digitali. Si tratta invero di pratiche che fino all'emanazione del regolamento europeo in questione venivano

[2] A. Gullo - G. Piccirilli, *Disinformazione e politiche pubbliche: una introduzione*, in *Diritto penale contemporaneo – Rivista Trimestrale*, 4, 2021, 248 ss.

[3] A. Gullo - G. Piccirilli, *ivi*, 249. In argomento v. anche A. Buratti, *Framing the Facebook Oversight Board: Rough Justice in the Wild Web?*, in questa *Rivista*, 2, 2022, 31 ss.

[4] Necessità che abbiamo ribadito anche all'esito del secondo ciclo della ricerca: v. il report del 2022, reperibile online in *esteri.it*.

[5] Per un primo inquadramento generale v. anche B. Tassone, *Riflessioni introduttive*, in *Diritto di internet*, 1, 2023, 3 ss. Nella letteratura internazionale v., ampiamente, anche per ulteriori riferimenti circa le varie implicazioni del nuovo regolamento, A. Turillazzi - M. Taddeo - L. Floridi - F. Casolari, *The digital services act: an analysis of its ethical, legal and social implications*, in *Law, Innovation and Technology*, 15(1), 2023, 83 ss.

[6] Cfr. il considerando 2 del regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), GU 2022 L 277/1 (corsivo nostro).

[7] V. sempre il considerando 2 del regolamento (UE) 2022/2065.

[8] Così il considerando 3 del regolamento (UE) 2022/2065.

svolte di fatto in assenza di una disciplina legislativa di riferimento, nonostante si trattasse e si tratti della prima (e soprattutto sovente anche unica) barriera "sanzionatoria" di contrasto alla diffusione della disinformazione in rete[9].

In linea generale, il primo effetto tangibile di questo regolamento su tali pratiche è determinato dall'art. 3, lett. t), che fornisce direttamente una definizione di «moderazione dei contenuti» –inquadrando così chiaramente, sul versante legislativo, il fenomeno che costituisce il *focus* di questa sezione del report – come «le attività, automatizzate o meno, svolte dai prestatori di servizi intermediari con il fine, in particolare, di individuare, identificare e contrastare contenuti illegali e informazioni incompatibili con le condizioni generali, forniti dai destinatari del servizio, comprese le misure adottate che incidono sulla disponibilità, sulla visibilità e sull'accessibilità di tali contenuti illegali o informazioni, quali la loro retrocessione, demonetizzazione o rimozione o la disabilitazione dell'accesso agli stessi, o che incidono sulla capacità dei destinatari del servizio di fornire tali informazioni, quali la cessazione o la sospensione dell'account di un destinatario del servizio»[10].

Il Capo III del regolamento, poi, disciplina in dettaglio tutta una serie di *due diligence obligations* relative, tra l'altro, proprio a tali attività di *private enforcement*, con un sistema di obblighi strutturato secondo vari "livelli" di intensità crescente in base al particolare destinatario degli stessi, dalla dimensione "base" delle previsioni applicabili a tutti i prestatori di servizi intermediari fino all'ultimo "gradino" concernente le più gravose regole applicabili alle piattaforme online e ai motori di ricerca di "dimensioni molto grandi". In particolare, il passaggio a ogni livello successivo comporta la sottoposizione dell'operatore all'obbligo di conformarsi ad alcune disposizioni ulteriori che si aggiungono (e *non* si sostituiscono) a quelle degli stadi precedenti[11].

Nei paragrafi successivi descriveremo, quindi, i principali contenuti di tali obblighi di diligenza, cercando di metterne in evidenza punti di forza e limiti anche alla luce degli esiti dell'indagine svolta durante i primi due cicli della presente ricerca, per poi delineare, in conclusione, alcune indicazioni di *policy*.

1.1. Obblighi in punto di definizione di termini e condizioni del servizio

Come noto, la sezione 1 del Capo III del DSA riguarda le disposizioni applicabili a

[9] Per una più ampia analisi, sia consentito rinviare ancora a E. Birritteri, *Punire la disinformazione*, cit., 304 ss.

[10] Lo stesso art. 3, poi, per quanto qui interessa fornisce sia, alla lett. h), la definizione di contenuto illegale come «qualsiasi informazione che, di per sé o in relazione a un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro conforme con il diritto dell'Unione, indipendentemente dalla natura o dall'oggetto specifico di tale diritto», sia, alla lett. u), quella di 'condizioni generali' come «tutte le clausole, comunque denominate e indipendentemente dalla loro forma, che disciplinano il rapporto contrattuale tra il prestatore dei servizi intermediari e il destinatario del servizio».

[11] Giustamente in dottrina si è subito parlato di approccio '*pyramid base*': v. M.L. Bixio, *Gli obblighi applicabili a tutti i prestatori di servizi intermediari, ai prestatori di servizi di* hosting *e ai fornitori di piattaforme* online *(Artt. 11-32 – Capo III, Sezioni, 1, 2, 3 e 4)*, in *Diritto di internet*, 1, 2023, 21.

tutti i prestatori di servizi intermediari.

La prima previsione che viene in considerazione in relazione all'oggetto di tale sezione della ricerca è senz'altro l'art. 14, che impone ai detti operatori di includere, con un linguaggio chiaro, semplice, comprensibile e adatto se del caso anche ai minori, nelle loro condizioni generali di erogazione del servizio, ogni informazione relativa a: a) tutte le politiche, le procedure e gli strumenti utilizzati nel moderare i contenuti immessi in rete dagli utenti, con informazioni specifiche sul «processo decisionale algoritmico e la verifica umana»[12]; c) le regole procedurali del loro sistema interno di gestione dei reclami[13].

È significativo notare come il legislatore europeo imponga a tali soggetti regolati, in definitiva, un obbligo di trasparenza rispetto alla necessità di informare i loro utenti sulle politiche connesse alla moderazione dei contenuti immessi in rete e sul funzionamento dei relativi mezzi di reclamo. Nulla si dice, quindi, sulle specifiche caratteristiche di dettaglio che tali procedure di *private enforcement* debbano avere, sui "connotati" dei processi di moderazione e su quelli, conseguenti, di reclamo da parte dell'utente rispetto alla decisione della piattaforma di imporre una restrizione sull'informazione immessa in rete. In tal senso, in questa previsione il DSA non impone modelli particolari.

Gli operatori, di conseguenza, rimangono sostanzialmente liberi di regolare nel modo da loro ritenuto più opportuno tanto i meccanismi di moderazione dei contenuti degli utenti, quanto i correlati strumenti di reclamo, dovendo però, nel farlo, come si legge al paragrafo 4 dell'art. 14 con una indicazione tanto generale quanto importante, agire «in modo diligente, obiettivo e proporzionato» e «tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte, compresi i diritti fondamentali dei destinatari del servizio, quali la libertà di espressione, la libertà e il pluralismo dei media, e altri diritti e libertà fondamentali sanciti dalla Carta»[14].

La scelta di *policy* qui fatta propria dal decisore eurounitario ci pare presenti aspetti positivi e alcune criticità.

Da un lato, invero, introdurre specifiche procedure di dettaglio sul piano della mo-

[12] Con una disposizione che evoca chiaramente i contenuti di cui all'art. 22 del GDPR, e l'esigenza quindi di una specifica forma di trasparenza in relazione ai principi ivi sanciti, che stabiliscono il diritto dell'interessato a non essere sottoposto a decisioni basate su trattamenti integralmente automatizzati che producano effetti che incidano sulla sua sfera giuridica, imponendo che tale automazione sia in tal senso parte di una procedura valutativa più ampia che, tra l'altro, preveda necessariamente l'intervento umano.

[13] I parr. 5 e 6 dell'art. 14 dettano poi alcune specificazioni di dettaglio ulteriori per le piattaforme e i motori di ricerca molto grandi «I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi forniscono ai destinatari dei servizi una sintesi concisa delle condizioni generali, di facile accesso e leggibile meccanicamente, compresi le misure correttive e i mezzi di ricorso disponibili, in un linguaggio chiaro e privo di ambiguità. Le piattaforme online di dimensioni molto grandi e i motori di ricerca online di dimensioni molto grandi ai sensi dell'articolo 33 pubblicano le loro condizioni generali nelle lingue ufficiali di tutti gli Stati membri in cui offrono i loro servizi». In linea generale, poi, la disposizione obbliga i prestatori a informare i destinatari di ogni significativa variazione in merito alle condizioni generali del servizio.

[14] È significativo evidenziare come ai sensi del considerando 47 del DSA, nel «progettare, applicare e far rispettare [le] restrizioni […] i prestatori di servizi intermediari dovrebbero inoltre tenere debitamente conto delle pertinenti norme internazionali in materia di tutela dei diritti umani, quali i principi guida delle Nazioni Unite su imprese e diritti umani».

derazione dei contenuti e dei reclami, valide per qualsiasi prestatore di servizi intermediari a prescindere dallo specifico mercato di riferimento, dal tipo di attività, dalla dimensione, secondo un modello *one size fits all*, sarebbe stato molto rischioso e, forse, controproducente, con il rischio di imporre oneri eccessivamente gravosi e non necessari[15]; anche il richiamo esplicito alla libertà di espressione e al pluralismo dei media, poi, appare molto importante specie sul piano del contrasto alla disinformazione, sensibilizzando gli operatori sulla necessità di adottare un approccio molto prudente e attento al rispetto dei diritti fondamentali nel disciplinare e applicare tali *policy* che, come ricordavamo, possono avere un impatto molto significativo su simili *fundamental rights* e generare un pericoloso e non auspicale *chilling effect*.

Dall'altro lato, però, pur senza legittimare inutili irrigidimenti burocratici, sarebbe stato a nostro avviso utile aggiungere qualche specificazione in più in merito ai "diritti di garanzia" minimali dell'utente sul piano delle misure che la piattaforma può disciplinare e adottare incidendo sui suoi diritti fondamentali (su tutti, dalla nostra prospettiva, la libertà di espressione). Nelle indicazioni di *policy* che avevamo formulato al termine dei precedenti due cicli della presente ricerca, ad esempio, avevamo menzionato sul punto, tra l'altro, come minimo «il principio di legalità delle violazioni e delle misure sanzionatorie/interdittive, con i relativi corollari della irretroattività, della tassatività/precisione delle previsioni punitive, e del divieto di analogia, nonché con una chiara definizione dei soggetti titolari della potestà di dettare tali regole; il principio di proporzionalità del trattamento sanzionatorio rispetto alla concreta gravità della violazione; il divieto di responsabilità oggettiva e l'affermazione del principio di colpevolezza, con la necessità di specificare l'elemento soggettivo (dolo o colpa) necessario per integrare la violazione»[16]. Come avremo modo di evidenziare a breve, su taluni di tali profili alcune disposizioni aggiuntive previste dal DSA e applicabili a certi operatori sembrano offrire soluzioni più soddisfacenti, ma tale prima previsione restituisce l'impressione di una non del tutto compiuta valorizzazione di profili di non secondaria importanza per una efficace protezione degli utenti. Del resto, sul versante specifico del contrasto alla disinformazione, è proprio su tali preliminari aspetti – *i.e.*, sulla determinazione dei principi di comportamento degli utenti e delle modalità d'uso del servizio, piuttosto che esclusivamente sul successivo *private enforcement* di tali regole – che i decisori pubblici sono chiamati a misurarsi con le più delicate ripercussioni dell'esercizio da parte delle *corporation* tecnologiche di tale potestà di autoregolare il dibattito pubblico e il confronto politico che si svolge sulle loro reti, con tutti i rischi di censura e di impatto negativo sui diritti fondamentali che ciò comporta[17].

[15] Su questi temi si veda diffusamente anche P. Leerssen, *An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation*, in *Computer Law & Security Review*, 48, 2023, 6.

[16] Vedi testualmente l'indicazione di *policy* n. 20, nella versione del report della ricerca del 2022, reperibile online in *esteri.it*.

[17] A.P. Heldt, *EU Digital Services Act: The White Hope of Intermediary Regulation*, in T. Flew - F.R. Martin (a cura di), *Digital Platform Regulation. Global Perspectives on Internet Governance*, Cham, 2022, 79.

1.2. Relazioni di trasparenza

La sezione 1 del Capo III del DSA prevede all'art. 15 un ulteriore obbligo di *due diligence* per tutti i prestatori di servizi intermediari[18], afferente al nostro ambito di interesse: si tratta del dovere di pubblicare, almeno una volta all'anno, «relazioni chiare e facilmente comprensibili sulle attività di moderazioni dei contenuti svolte durante il periodo di riferimento».

Tali relazioni devono comprendere una serie di informazioni su, tra l'altro: *a)* le attività di moderazione di contenuti avviate di propria iniziativa anche mediante l'uso di strumenti automatizzati; per qualsiasi utilizzo di questi ultimi nelle attività di moderazione, peraltro, si devono fornire dettagli concernenti «la descrizione qualitativa, la descrizione delle finalità precise, gli indicatori di accuratezza e il possibile tasso di errore degli strumenti automatizzati utilizzati nel perseguimento di tali scopi e le eventuali garanzie applicate»; *b)* le misure implementate per fornire una specifica formazione e assistenza alle persone dell'organizzazione incaricate di svolgere tale attività di *private enforcement*; *c)* il numero e il tipo di "sanzioni" irrogate agli utenti avuto riguardo a ogni restrizione all'uso del servizio, con la necessità, tra l'altro, di classificare e differenziare tali informazioni in base alle diverse tipologie di contenuto illegale o alle specifiche regole interne della piattaforma violate, nonché con riferimento al metodo di rilevamento dell'inosservanza; *d)* il numero di reclami ricevuti[19]. Per le piattaforme online e i motori di ricerca "di dimensioni molto grandi", in linea con gli obblighi aggiuntivi per loro previsti[20], si prevedono altresì misure ancor più stringenti in merito ai contenuti e alle tempistiche di tale relazione[21].

---

[18] Il par. 2 dell'art. 15 peraltro stabilisce che «Il paragrafo 1 del presente articolo non si applica ai prestatori di servizi intermediari che si qualificano come microimprese o piccole imprese come definite nella raccomandazione 2003/361/CE e che non sono piattaforme online di dimensioni molto grandi a norma dell'articolo 33 del presente regolamento».

[19] In base alle lett. a) e b) del par. 1 dell'art. 15, inoltre, occorre indicare «a) per i prestatori di servizi intermediari, il numero di ordini ricevuti dalle autorità degli Stati membri, compresi gli ordini emessi a norma degli articoli 9 e 10, classificati in base al tipo di contenuti illegali in questione, lo Stato membro che ha emesso l'ordine e il tempo medio necessario per informare l'autorità che ha emesso l'ordine o qualsiasi altra autorità specificata nell'ordine in merito al suo ricevimento e per dare seguito allo stesso; b) per i prestatori di servizi di memorizzazione di informazioni, il numero di segnalazioni presentate a norma dell'articolo 16, classificate in base al tipo di contenuto illegale presunto di cui trattasi, il numero di segnalazioni presentate da segnalatori attendibili, nonché eventuali azioni intraprese in applicazione delle segnalazioni, specificando se l'azione sia stata avviata in virtù di disposizioni normative oppure delle condizioni generali del prestatore, il numero di segnalazioni trattate utilizzando strumenti automatizzati e il tempo mediano necessario per intraprendere l'azione». Rispetto ai reclami, poi, la lett. d) stabilisce che è necessario anche menzionare «per i fornitori di piattaforme online, conformemente all'articolo 20, la base di tali reclami, le decisioni adottate in relazione a tali reclami, il tempo mediano necessario per adottare tali decisioni e il numero di casi in cui tali decisioni sono state revocate». Ai sensi dell'art. 24 del DSA, tra l'altro, i fornitori di piattaforme online devono includere alcune informazioni aggiuntive in tale relazione, tra cui il numero di controversie sottoposte all'esame degli organismi di risoluzione extragiudiziale e il numero di sospensioni imposte *ex* art. 23 DSA.

[20] Sui quali ci soffermeremo nel dettaglio *infra* (par. 4 e ss. del presente capitolo).

[21] L'art. 42 del DSA stabilisce, infatti, che questi operatori debbano pubblicare, in almeno una delle lingue ufficiali degli Stati membri, «le relazioni di cui all'articolo 15 al più tardi entro due mesi dalla data di applicazione di cui all'articolo 33, paragrafo 6, secondo comma, e successivamente almeno ogni sei mesi», specificando «oltre alle informazioni di cui all'articolo 15 e all'articolo 24, paragrafo 1: a) le risorse

La commissione, inoltre, potrà adottare «atti di esecuzione per stabilire modelli relativi alla forma, al contenuto e ad altri dettagli delle relazioni a norma del paragrafo 1 del presente articolo, compresi periodi di comunicazione armonizzati», diffondendo quindi *best practice* operative e modelli standard di riferimento che potranno essere di concreto ausilio agli operatori per adeguarsi a tali obblighi di conformità.
Si tratta senz'altro di una previsione condivisibile ove l'obbligo di trasparenza imposto alle piattaforme muove dalla prospettiva *in the books* dell'art. 14 a quella, per così dire, *in action*, imponendosi una *disclosure* anche sul modo in cui le regole autonormate dalle piattaforme sull'attività di moderazione dei contenuti sono effettivamente applicate in concreto, nella quotidiana realtà operativa dell'organizzazione.
Ciò sembra poter consentire agli organi di *enforcement* di accedere a informazioni che hanno indubbiamente un peso specifico significativo per valutare se gli obblighi definiti dall'art. 14 del DSA siano effettivamente rispettati, pur rimanendo naturalmente ferme le perplessità sul margine di libero apprezzamento lasciato alle piattaforme nel definire, a monte, tali regole del gioco. Si tratta invero di un potere che non pare poter essere ridotto dal dovere, a valle, di pubblicare relazioni in merito alla concreta applicazione di misure costruite secondo una discrezionalità che rimane, come abbiamo rilevato, certamente ampia per larghi tratti.

2. Disposizioni aggiuntive applicabili ai prestatori di servizi di memorizzazione di informazioni, comprese le piattaforme online

Come osservato in apertura il DSA prevede una serie di doveri di diligenza a intensità crescente per gli operatori, che variano a seconda del tipo di soggetto regolato[22]; il pas-

umane dedicate dal fornitore di piattaforme online di dimensioni molto grandi alla moderazione dei contenuti in relazione al servizio offerto nell'Unione, suddivise per ciascuna lingua ufficiale applicabile degli Stati membri anche per il rispetto degli obblighi di cui agli articoli 16 e 22, nonché per il rispetto degli obblighi di cui all'articolo 20; b) le qualifiche e le competenze linguistiche delle persone che svolgono le attività di cui alla lettera a), nonché la formazione e il sostegno forniti a tale personale; c) gli indicatori di accuratezza e le relative informazioni di cui all'articolo 15, paragrafo 1, lettera e), suddivisi per ciascuna lingua ufficiale degli Stati membri», nonché ulteriori informazioni concernenti il numero medio mensile dei destinatari del servizio, anche per ciascun Stato membro. Specifici obblighi di pubblicazione e comunicazione aggiuntivi si riferiscono poi, ai sensi dei parr. 4 e 5 dell'art. 42 del DSA, agli *independent audit* cui tali soggetti, come vedremo (cfr. infra par. 4.4.), devono sottoporsi, prevedendosi tra l'altro che qualora «un fornitore di piattaforme online di dimensioni molto grandi o di motori di ricerca online di dimensioni molto grandi ritenga che la pubblicazione di informazioni a norma del paragrafo 4 possa comportare la divulgazione di informazioni riservate di tale fornitore o dei destinatari del servizio, comportare notevoli vulnerabilità per la sicurezza del suo servizio, compromettere la sicurezza pubblica o danneggiare i destinatari, può rimuovere tali informazioni dalle relazioni disponibili al pubblico. In tal caso il fornitore trasmette le relazioni complete al coordinatore dei servizi digitali del luogo di stabilimento e alla Commissione, corredate di una spiegazione dei motivi alla base della rimozione delle informazioni dalle relazioni disponibili al pubblico».

[22] G. Buttarelli, *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche*, in *Giornale di diritto amministrativo,* 1, 2023, 116 ss. Autorevole dottrina rileva inoltre come, tra obblighi di diligenza privati e responsabilità pubbliche di *enforcement*, il DSA preveda un sistema "a rete" di poteri di vigilanza e controllo: L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Rivista trimestrale di diritto pubblico*, 4, 2022, 1108.

saggio a ogni nuovo livello comporta l'applicazione di obblighi aggiuntivi, che vanno a sommarsi a quelli dei "piani" precedenti. Il primo di tali "strati" di *obligation* aggiuntive è costituito dalle disposizioni della sezione II del capo III del DSA, concernente le regole applicabili ai prestatori di servizi di "memorizzazione di informazioni", comprese le piattaforme online. Per quanto qui interessa assumono in particolare rilievo gli artt. 16 e 17 del DSA, sui quali quindi soffermeremo subito la nostra attenzione.

2.1. Meccanismo di *notice and action*

La prima rilevante previsione è quella dell'art. 16 del DSA, che impone a tutti i prestatori di servizi di memorizzazione di predisporre meccanismi di «facile accesso e uso» per «consentire a qualsiasi persona o ente» di notificare la presenza «nel loro servizio di informazioni specifiche che tale persona o ente ritiene costituiscano contenuti illegali», con la possibilità di presentare «segnalazioni esclusivamente per via elettronica». Tali operatori, poi, dovranno predisporre misure idonee a facilitare le segnalazioni che appaiano «sufficientemente precise e adeguatamente motivate», qualificandosi in sostanza come tali quelle che presentino una serie di contenuti di dettaglio descritti analiticamente dal par. 2 dell'art. 16[23].

In tale disposizione, poi, il DSA, si occupa di fornire alcune indicazioni ulteriori, sia di carattere più generale che di dettaglio, circa gli obblighi procedurali a carico del prestatore e i diritti previsti per gli utenti interessati.

Dal primo punto di vista, infatti, in parte ricalcando quanto l'art. 14 precisa rispetto alla definizione di termini e condizioni, si prevede l'obbligo per i detti prestatori di prendere in carico simili segnalazioni e di adottare le decisioni in merito alle informazioni cui queste si riferiscono «in modo tempestivo, diligente, non arbitrario e obiettivo», fornendo altresì informazioni specifiche sull'eventuale uso di strumenti automatizzati nel trattare e assumere provvedimenti rispetto alle stesse.

Dal secondo punto di vista, poi, delineando un livello basilare e minimo di "diritti procedurali", si prevede che l'operatore digitale debba informare, sempre «senza indebito ritardo», il segnalatore (che può essere sia una persona fisica che un ente, che abbia fornito il proprio contatto «elettronico») sia del ricevimento della segnalazione, sia della decisione presa in merito, fornendo contestualmente ogni informazione circa i ricorsi disponibili per contestare il provvedimento del prestatore.

È significativo notare, inoltre, come le segnalazioni in questione siano in grado di dispiegare effetti anche rispetto al regime di responsabilità del *provider,* nella misura in cui

[23] E cioè «a) una spiegazione sufficientemente motivata dei motivi per cui la persona o l'ente presume che le informazioni in questione costituiscano contenuti illegali; b) una chiara indicazione dell'ubicazione elettronica esatta di tali informazioni, quali l'indirizzo o gli indirizzi URL esatti e, se necessario, informazioni supplementari che consentano di individuare il contenuto illegale adeguato al tipo di contenuto e al tipo specifico di servizio di memorizzazione di informazioni; c) il nome e l'indirizzo di posta elettronica della persona o dell'ente che presenta la segnalazione, tranne nel caso di informazioni che si ritiene riguardino uno dei reati di cui agli articoli da 3 a 7 della Direttiva 2011/93/UE (n.d.r. gli illeciti penali relativi agli abusi, allo sfruttamento sessuale dei minori e alla pornografia minorile); d) una dichiarazione con cui la persona o l'ente che presenta la segnalazione conferma la propria convinzione in buona fede circa l'esattezza e la completezza delle informazioni e delle dichiarazioni ivi contenute».

il paragrafo 3 dell'art. 16 sancisce che, ove tali *notices* consentano all'organizzazione di prendere contezza dell'illegalità del contenuto «senza un esame giuridico dettagliato», «si considera» che queste permettono all'operatore di acquisire una conoscenza effettiva dell'illegalità dell'attività o dell'informazione veicolata tramite i suoi servizi, con tutto ciò che ne consegue a norma dell'art. 6 circa la *hosting provider liability*[24].

La previsione dell'art. 16 è particolarmente opportuna nella misura in cui consente di "istituzionalizzare" un meccanismo di cruciale importanza come quello delle segnalazioni, con cui enti e persone fisiche possono "stimolare" gli operatori digitali a porre in essere in modo più efficace la loro attività di *private enforcement*, anche in un certo senso affiancandoli e supportandoli in procedure senz'altro molto onerose già sul piano gestionale e organizzativo. Del resto, *ad impossibilia nemo tenetur*, sicché non potremmo certo aspettarci/pretendere che i soggetti regolati in questione siano in grado, da soli, di identificare ogni contenuto illegale condiviso tramite i loro sevizi.

È molto importante evidenziare, però, come tale meccanismo di *notice and action* debba essere obbligatoriamente predisposto solo per ciò che concerne la segnalazione di attività e contenuti *illegali*[25] e non già, stando alla "lettera" dell'art. 16, per quelli meramente lesivi delle condizioni generali d'uso del servizio o c.d. standard della *community*. Fermo restando che le piattaforme, naturalmente, potranno pur sempre spontaneamente estendere il raggio applicativo di tali procedure, consentendo di attivarle anche per segnalare la presenza di contenuti non illegali, ma semplicemente lesivi delle condizioni d'uso del servizio quanto ad attività che non possono essere svolte sui loro servizi, bisognerebbe forse interrogarsi sulla condivisibilità o meno di tale scelta di regolazione e della decisione del legislatore europeo di non estendere l'adozione obbligatoria di simili procedure anche alle informazioni in parola.

Specie per ciò che concerne il contrasto alla disinformazione, infatti, molto spesso alcune modalità d'utilizzo del servizio (si pensi alla interazione tra più *account* al fine di aumentare artificiosamente la visibilità di certe notizie, o all'uso coordinato di *fake account* o *bot* automatici, etc.) non possono dirsi di per sé – o comunque non possono sempre agevolmente qualificarsi – come illegali; lo stesso vale per molte affermazioni false veicolate in campagne anche coordinate di disinformazione che, secondo quanto abbiamo avuto modo di osservare ampiamente nei precedenti cicli della ricerca, non hanno sovente alcuna rilevanza penale o, in generale, carattere di illiceità per l'ordinamento giuridico[26].

A volte, però, si tratta di informazioni rispetto alle quali la piattaforma può legittimamente decidere di applicare delle restrizioni (da quelle più *soft* concernenti l'utilizzo di

[24] In argomento rinviamo integralmente alla disamina svolta in dettaglio nel primo saggio della presente sezione (di L. D'Agostino, *Disinformazione e obblighi di* compliance *degli operatori del mercato digitale alla luce del nuovo* Digital Services Act). Sul tema v. anche, di recente, S. Braschi, *Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli* Internet Service Provider*?*, in *Diritto penale e processo*, 3, 2023, 367 ss.

[25] Osserva M.L. Bixio, *Gli obblighi applicabili a tutti i prestatori di servizi*, cit., 23, che «la struttura *pyramid base*, tra i diversi tipi di servizi intermediari, ammette solo per l'*hosting* la segnalazione da parte di un soggetto privato e, per conseguenza, l'art. 9 tratta solo degli ordini (e non delle segnalazioni) rivolte ai prestatori di servizi intermediari».

[26] Per ogni riferimento v. E. Birritteri, *Punire la disinformazione*, cit., 316 ss.

banner con rinvio ad *alert* di *fact-checkers* indipendenti, fino a misure più incisive come la riduzione di visibilità o la rimozione del contenuto lesivo degli standard della *community*), per cui simili meccanismi di *notice and action* potrebbero rivestire particolare utilità, ferma restando naturalmente la 'generale 'esigenza, sopra evidenziata, che le piattaforme disciplinino l'utilizzo di tale potere "sanzionatorio" nel rispetto dei minimali principi di garanzia propri di qualsiasi paradigma disciplinare/punitivo, anche in ambito privato.

2.2. Obbligo di motivazione sulle misure di moderazione dei contenuti

La seconda previsione della sezione in analisi del DSA (art. 17) riguarda l'obbligo per i prestatori di *hosting services* di fornire ai destinatari del servizio, salvo che si tratti di contenuti commerciali ingannevoli ad ampia diffusione[27] o dell'esecuzione di ordini di autorità pubbliche *ex* art. 9 DSA, «una motivazione chiara e specifica»[28] su una serie di "sanzioni" applicate in sede di moderazione dei contenuti e nominalmente indicate dal par. 1 della disposizione (dalla semplice riduzione di visibilità dell'informazione, alla sospensione o cessazione della prestazione del servizio, fino alla chiusura dell'*account*)[29].
Il par. 3, inoltre, offre ulteriori e importanti dettagli sul contenuto specifico dell'obbligo di motivazione che grava su simili operatori.
Anzitutto, infatti, occorre chiarire la tipologia di sanzione che è stata irrogata, specificandone la portata territoriale e la durata.
Bisogna, poi, indicare «i fatti e le circostanze su cui si basa la decisione» di applicare la restrizione del servizio, specificando, ma solo «ove opportuno», se la sanzione sia stata applicata all'esito di una segnalazione pervenuta tramite il meccanismo di *notice and action* dell'art. 16 o in virtù di indagini volontarie intraprese di propria iniziativa dall'organizzazione, nonché – ma solo, anche qui, «ove strettamente necessario» – l'identità stessa del notificante. Queste ultime clausole di riserva attribuiscono un notevole margine di apprezzamento alle piattaforme e non potrà che essere l'*enforcement* concreto dal

[27] Qualche chiarimento sul punto è offerto dal considerando 55 del DSA, ove si legge che «L'obbligo di fornire una motivazione non dovrebbe tuttavia applicarsi ai contenuti commerciali ingannevoli ad ampia diffusione diffusi attraverso la manipolazione intenzionale del servizio, in particolare l'utilizzo non autentico del servizio, come l'utilizzo di bot o account falsi o altri usi ingannevoli del servizio».

[28] Il par. 4 della previsione aggiunge che le «Le informazioni fornite dai prestatori di servizi di memorizzazione di informazioni a norma del presente articolo devono essere chiare e facilmente comprensibili e il più possibile precise e specifiche tenuto conto delle circostanze del caso. In particolare le informazioni devono essere tali da consentire ragionevolmente al destinatario del servizio interessato di sfruttare in modo effettivo le possibilità di ricorso di cui al paragrafo 3, lettera f)».

[29] Nello specifico, il par. 1 dell'art. 17 DSA prevede l'obbligo di fornire tale motivazione rispetto alle seguenti misure: «a) eventuali restrizioni alla visibilità di informazioni specifiche fornite dal destinatario del servizio, comprese la rimozione di contenuti, la disabilitazione dell'accesso ai contenuti o la retrocessione dei contenuti; b) la sospensione, la cessazione o altra limitazione dei pagamenti in denaro; c) la sospensione o la cessazione totale o parziale della prestazione del servizio; d) la sospensione o la chiusura dell'account del destinatario del servizio». Si specifica al par. 2, tra l'altro, che tale previsione «si applica solo se le pertinenti coordinate elettroniche sono note al prestatore» e «al più tardi dalla data a partire dalla quale la restrizione è imposta, indipendentemente dal motivo o dal modo in cui è imposta».

DSA a chiarirne effettivamente la portata. Ci sembra, comunque, si possa leggere tra le righe la volontà del legislatore eurounitario di tutelare i segnalanti, lasciando però agli operatori digitali il delicato compito di operare un complesso bilanciamento tra tali esigenze di protezione e i "diritti di difesa" dell'utente che ha subito la restrizione imposta dalla piattaforma.

Occorre, inoltre, chiarire se la decisione sia stata presa in virtù dell'illegalità del contenuto o della sua incompatibilità con le condizioni generali d'uso del servizio (quindi, con le regole autonormate dalla piattaforma circa i c.d. standard della *community*), in entrambi i casi indicando la specifica base giuridica o la clausola contrattuale "interna" che si assume violata e i motivi per cui l'informazione o il contenuto vengono considerati in contrasto con tali previsioni.

Infine, con ulteriori due indicazioni, come visto, ricorrenti in tutto il DSA, si prevede l'obbligo per il prestatore di chiarire se la decisione sia stata presa utilizzando strumenti automatizzati anche, se del caso, per individuare il contenuto oggetto del provvedimento "sanzionatorio", nonché di fornire «informazioni chiare e di facile comprensione sui mezzi di ricorso a disposizione del destinatario del servizio in relazione alla decisione, in particolare […] attraverso i meccanismi interni di gestione dei reclami, la risoluzione extragiudiziale delle controversie e il ricorso per via giudiziaria».

L'art. 17 del DSA riveste, come ben può intuirsi, una primaria importanza rispetto al funzionamento concreto delle dinamiche di *private enforcement* degli operatori digitali.

Infatti, nella fase di autonormazione a monte, come abbiamo rilevato, i soggetti regolati mantengono un significativo margine di apprezzamento nell'individuare le informazioni o i contenuti (anche sul piano della lotta alla disinformazione) che possono essere veicolati o meno tramite le loro piattaforme, al netto della "sintetica" menzione della necessità di esercitare tale potestà di autoregolazione «in modo diligente, obiettivo e proporzionato» e «tenendo debitamente conto dei […] diritti e [delle] libertà fondamentali sanciti dalla Carta». Nella fase di *enforcement* a valle di tali regole autonormate, invece, l'articolo in commento appare più "sensibile" alle esigenze sia di dettagliare maggiormente, e non solo con clausole di carattere generale, gli obblighi degli operatori, sia di rafforzare e specificare con più analiticità i diritti e le garanzie procedurali minime per gli utenti che subiscono simili misure para-punitive[30].

L'ampiezza dell'obbligo motivazionale imposto ai soggetti regolati, infatti, pur ponendo in capo ad essi significativi oneri gestionali e organizzativi, appare una soluzione necessaria in considerazione dei diritti fondamentali su cui simili attività possono significativamente incidere, oltre a fornire una base di informazioni di partenza indispensabile per l'utente che voglia avvalersi degli strumenti di reclamo "interni" o "esterni" effettivamente disponibili a tutela della sua posizione.

In parte qua, allora, e anche tenuto conto del più limitato novero di operatori cui, come

[30] P. Leerssen, *An end to shadow banning?*, cit., 8, che osserva anche in chiave critica come «*the DSA's approach is inflexible in that it bundles all relevant due process rights – notice, explanation and appeals – into the singular concept of a 'moderation action'. In practice there may be a large set of edge-cases where integral explanation and/or appeal could be onerous in terms of costs, or too sensitive in terms of security, but where a bare notice right could still be of substantial value as a bulwark against shadow banning and as a minimal precondition for legal and social accountability. In this light, the DSA's attempt at balancing is somewhat rudimentary, and in future may benefit from further refinement, such as by incorporating more factors into the shadow banning calculus and unbundling notice safeguards from other aspects of due process*».

visto, si applica tale disposizione, il DSA opera un bilanciamento tutto sommato ragionevole tra tali interessi contrapposti, pure in considerazione del significativo squilibrio tra i "poteri" contrattuali delle parti[31].

3. Disposizioni aggiuntive applicabili alle piattaforme online

Nella struttura a intensità crescente delle *due diligence obligation* del DSA, la sezione III del Capo III del regolamento rafforza ulteriormente gli oneri di *compliance* gravanti sui più importanti *player* del mercato digitale, introducendo una serie di disposizioni aggiuntive applicabili alle piattaforme online, che, come noto, specie nel contrasto alla disinformazione, costituiscono i naturali interlocutori di qualsiasi strategia di regolazione del fenomeno.

Per quanto qui interessa, in particolare, vengono in rilievo le previsioni di cui agli artt. 20, 21 e 22 del DSA, applicabili a tutte le piattaforme online ad eccezione di quelle qualificabili come microimprese o piccole imprese ai sensi della Raccomandazione (CE) 2003/361, per quanto tale deroga non operi rispetto a quelli che, anche tra questi ultimi operatori, vengano designati come «piattaforme online di dimensioni molto grandi a norma dell'articolo 33, indipendentemente dal fatto che si qualifichino come microimprese o piccole imprese»[32].

3.1. Il sistema interno di gestione dei reclami

La prima *due diligence obligation* aggiuntiva per le piattaforme online consiste nell'obbligo di fornire ai propri utenti, comprese persone o enti che presentano una segnalazione, per almeno sei mesi[33] dalla decisione sulla segnalazione o dall'applicazione della "sanzione" nell'ambito dell'attività di moderazione di contenuti illegali o contrari alle

[31] Sul problema, in tali contesti, dell'"asimmetria delle posizioni' degli attori in campo v. B. Carotti, *La politica europea sul digitale: ancora molto rumore*, in *Rivista trimestrale di diritto pubblico*, 4, 2022, 998. Diffusamente cfr. anche G. Alpa, *Sul potere contrattuale delle piattaforme digitali*, in *Contratto delle imprese*, 2022, 721 ss.

[32] In particolare, l'art. 19 del DSA stabilisce in dettaglio che «1. La presente sezione, ad eccezione dell'articolo 24, paragrafo 3, non si applica ai fornitori di piattaforme online che si qualificano come microimprese o piccole imprese quali definite nella raccomandazione 2003/361/CE. La presente sezione, ad eccezione dell'articolo 24, paragrafo 3, non si applica ai fornitori di piattaforme online che si sono precedentemente qualificati come microimprese o piccole imprese quali definite nella raccomandazione 2003/361/CE nel corso dei 12 mesi successivi alla perdita di tale qualifica a norma dell'articolo 4, paragrafo 2, della medesima raccomandazione, tranne quando sono piattaforme online di dimensioni molto grandi ai sensi dell'articolo 33. 2. In deroga al paragrafo 1 del presente articolo, la presente sezione si applica ai fornitori di piattaforme online che sono stati designati come piattaforme online di dimensioni molto grandi a norma dell'articolo 33, indipendentemente dal fatto che si qualifichino come microimprese o piccole imprese».

[33] Il par. 2 dell'art. 20 precisa che il «periodo di almeno sei mesi di cui al paragrafo 1 del presente articolo decorre dal giorno in cui il destinatario del servizio è stato informato della decisione a norma dell'articolo 16, paragrafo 5, o dell'articolo 17».

condizioni generali del servizio[34], «l'accesso a un sistema interno di gestione dei reclami efficace, che consenta loro di presentare per via elettronica e gratuitamente reclami contro la decisione presa dal fornitore della piattaforma», che sia di «facile accesso e uso» e tale da consentire e agevolare «la presentazione di reclami sufficientemente precisi e adeguatamente motivati».

Anche in questo caso, sulla scorta di quanto già rilevato con riferimento all'art. 14 del DSA in punto di definizione di termini e condizioni del servizio, e in qualche modo a differenza dell'art. 17, il DSA non fornisce un *set* preciso di regole di dettaglio circa il funzionamento specifico di tali procedure interne di reclamo e sui correlati diritti procedurali specie del destinatario della "sanzione" irrogata dalla piattaforma.

Il par. 4 dell'art. 20, invero, si "limita" a sancire l'obbligo delle piattaforme online di gestire i reclami presentati tramite il loro sistema interno in modo «in modo tempestivo, non discriminatorio, diligente e non arbitrario», di ritirare la propria decisione ove il reclamo contenga «sufficienti motivi per indurre il fornitore a ritenere» che la decisione presa sia infondata, di comunicare senza indebito ritardo ai reclamanti la loro «decisione motivata» in merito al reclamo presentato nonché i mezzi ulteriori di ricorso a loro disposizione, nonché – in misura qui forse più significativa – la necessità che il ricorsi interni in questione vengano decisi «con la supervisione di personale adeguatamente qualificato e non avvalendosi esclusivamente di strumenti automatizzati» (essendo, del resto, costante l'attenzione rivolta dal DSA al rispetto dell'art. 22 del GDPR[35]).

Anche qui, dunque, alle piattaforme, fermi restando questi principi di fondo, viene lasciata ampia potestà di disciplinare nel modo ritenuto più opportuno il funzionamento concreto di tali procedure e sistemi interni di reclamo.

Pure in tal caso, però, senza legittimare formalismi eccessivi e non necessari, sarebbe stato auspicabile fornire indicazioni di maggiore dettaglio circa le garanzie procedurali minime a tutela di utenti che si trovino di fronte a decisioni capaci di incidere in modo significativo sui loro diritti fondamentali, avuto naturalmente particolare riguardo, nel settore del contrasto alla disinformazione, alla libertà di espressione.

Nei cicli precedenti della ricerca, del resto, avevamo osservato come proprio le procedure e le regole di funzionamento dei sistemi interni di reclamo fossero un ambito in cui le piattaforme online fanno spesso registrare un ridotto livello di trasparenza, e come fosse necessario costruire una cornice pubblica di regole del gioco tali da obbligare le piattaforme a garantire un livello minimo di "diritti di difesa" a tutela degli utenti, tra cui, ad esempio, il diritto al contraddittorio preventivo, la garanzia di sufficiente autonomia e indipendenza (anche rispetto alla distribuzione interna dei

[34] In particolare, il par. 1 dell'art. 20 del DSA menziona: «a) le decisioni che indicano se rimuovere le informazioni o disabilitare l'accesso alle stesse o se limitarne la visibilità; b) le decisioni che indicano se sospendere o cessare in tutto o in parte la prestazione del servizio ai destinatari; c) le decisioni che indicano se sospendere o cessare l'account dei destinatari; d) le decisioni che indicano se sospendere, cessare o limitare in altro modo la capacità di monetizzare le informazioni fornite dai destinatari».

[35] Sul tema, in generale, dei trattamenti automatizzati anche con riferimento a quest'ultima disposizione, v., nella dottrina penalistica, anche per più ampi riferimenti, tra gli altri: L. D'Agostino, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al d.lgs. 10 agosto 2018, n. 101,* in *Archivio penale,* 1, 17 ss.; G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Diritto penale contemporaneo – Rivista Trimestrale*, 4, 2020, 75 ss.

poteri dell'organizzazione) dei soggetti deputati a irrogare la sanzione e a decidere sui connessi reclami, il diritto di richiedere, già a livello interno, un ulteriore riesame della decisione[36].

Pur non potendosi certamente imporre generali modelli standard secondo un analitico livello di dettaglio, insomma, l'impressione anche su questo versante è quella di un percorso che, pur avendo condivisibilmente istituzionalizzato tali meccanismi e correttamente sancito in linea generale l'obbligo delle piattaforme di agire in modo non discriminatorio e arbitrario e secondo diligenza anche nella gestione dei reclami interni, poteva essere ancora perfezionato nella direzione della più efficace tutela dei diritti degli utenti[37].

3.2. La risoluzione extragiudiziale delle controversie

L'art. 21 del DSA stabilisce che gli utenti e coloro che hanno presentato segnalazioni hanno il diritto di scegliere, rispetto a qualsiasi controversia inerente alle stesse decisioni delle piattaforme menzionate dal par. 1 dell'art. 20 del DSA, compresi i «reclami che non è stato possibile risolvere mediante il sistema interno di gestione dei reclami di cui a tale articolo», «qualunque organismo di risoluzione extragiudiziale delle controversie» certificato ai sensi del par. 3 dell'art. 21, che subordina l'ottenimento di tale certificazione, attribuita dal coordinatore dei servizi digitali dello Stato membro, al soddisfacimento di requisiti dettagliatamente descritti e volti principalmente ad assicurare la competenza, l'imparzialità e l'indipendenza di simili organismi e l'adozione da parte loro di «regole procedurali chiare ed eque»[38].

---

[36] E. Birritteri, *Punire la disinformazione*, cit., 322 ss.

[37] In dottrina, invero, nei primi commenti al DSA è subito emerso un primo dibattito anche su questi aspetti: cfr. F. G'sell, *The Digital Services Act: A General Assessment*, in A. von Ungern-Sternberg (a cura di), *Content Regulation in the European Union. The Digital Services Act*, Trier, 2023, 95.

[38] In particolare, il par. 3 dell'art. 21 del DSA prevede che «Il coordinatore dei servizi digitali dello Stato membro in cui è stabilito l'organismo di risoluzione extragiudiziale delle controversie certifica tale organismo, su sua richiesta, per un periodo massimo di cinque anni rinnovabile, se il medesimo ha dimostrato di soddisfare tutte le condizioni seguenti: a) è imparziale e indipendente, anche sul piano finanziario, dai fornitori di piattaforme online e dai destinatari del servizio prestato dai fornitori di piattaforme online, ivi compresi le persone o gli enti che hanno presentato segnalazioni; b) dispone delle competenze necessarie, in relazione alle questioni che sorgono in uno o più ambiti specifici relativi ai contenuti illegali o in relazione all'applicazione e all'esecuzione delle condizioni generali di uno o più tipi di piattaforme online, per consentire a tale organismo di contribuire efficacemente alla risoluzione di una controversia; c) i suoi membri sono retribuiti secondo modalità non legate all'esito della procedura; d) la risoluzione extragiudiziale delle controversie che offre è facilmente accessibile attraverso le tecnologie di comunicazione elettronica e prevede la possibilità di avviare la risoluzione delle controversie e di presentare i necessari documenti giustificativi online; e) è in grado di risolvere le controversie in modo rapido, efficiente ed efficace sotto il profilo dei costi e in almeno una delle lingue ufficiali delle istituzioni dell'Unione; f) la risoluzione extragiudiziale delle controversie che offre avviene secondo regole procedurali chiare ed eque che sono facilmente e pubblicamente accessibili e conformi al diritto applicabile, compreso il presente articolo. Ove opportuno il coordinatore dei servizi digitali specifica nel certificato: a) le questioni concrete cui si riferisce la competenza dell'organismo, a norma del primo comma, lettera b); e b) la lingua o le lingue ufficiali delle istituzioni dell'Unione in cui l'organismo è in grado di risolvere le controversie, a norma del primo comma, lettera e)». Il par. 4 della medesima previsione aggiunge che «I coordinatori dei servizi digitali elaborano ogni due anni

I fornitori di piattaforme online hanno l'obbligo di rendere edotti chiaramente i propri utenti sulle possibilità di avere accesso a tali strumenti di risoluzione extragiudiziale delle controversie, facendo sì che tali informazioni siano «agevolmente accessibili sulla loro interfaccia online», pur restando impregiudicato, ai sensi del par. 1 dell'art. 21, «il diritto del destinatario del servizio in questione di avviare, in qualsiasi fase, procedimenti per contestare tali decisioni da parte dei fornitori di piattaforme online dinanzi a un organo giurisdizionale conformemente al diritto applicabile».

Del resto, la disposizione è ben chiara nel prevedere che tali organismi di risoluzione extragiudiziale non abbiano il potere di imporre una decisione «vincolante per le parti» e che le stesse piattaforme online possano legittimamente rifiutarsi di adirli «qualora una controversia riguardante le stesse informazioni e gli stessi motivi di presunta illegalità o incompatibilità dei contenuti sia già stata risolta».

Sul piano procedurale, si prevede che le parti «adiscono in buona fede» l'organismo in questione, che deve mettere a loro disposizione[39] il proprio provvedimento, come visto, non vincolante, entro 90 giorni dal ricevimento del reclamo, con la possibilità di prorogare il termine per definire il procedimento di oltre 90 giorni al massimo in caso di controversie molto complesse.

Per ciò che concerne i risarcimenti e i costi della lite, tra l'altro, è evidente il *favor* legislativo nei confronti del reclamante, alla luce del noto squilibrio contrattuale e di poteri tra le parti in causa in questi contesti, specie nella misura in cui si prevede che gli utenti debbano poter accedere «gratuitamente, o per un importo simbolico» a tali meccanismi[40], nonché che, a differenza delle piattaforme, non debbano farsi carico dei e «diritti e [del]le altre spese che il fornitore della piattaforma online ha sostenuto o deve sostenere in relazione alla risoluzione della controversia, a meno che l'organismo di risoluzione extragiudiziale delle controversie non ritenga che detto destinatario abbia agito manifestamente in mala fede».

Tale previsione, al netto della natura non vincolante delle decisioni degli organismi in parola, ci pare rivesta in definitiva una indubbia importanza nella misura in cui offre agli utenti dei servizi digitali una ulteriore alternativa per tutelare la propria posizione,

una relazione sul funzionamento degli organismi di risoluzione extragiudiziale delle controversie da essi certificati. In particolare, tale relazione: a) elenca il numero di controversie che ciascun organismo di risoluzione extragiudiziale delle controversie certificato ha ricevuto ogni anno; b) indica l'esito delle procedure avviate dinanzi a tali organi e il tempo medio necessario per risolvere le controversie; c) individua e spiega eventuali carenze sistemiche o settoriali o difficoltà incontrate in relazione al funzionamento di tali organismi; d) individua le migliori prassi relative a tale funzionamento; e) formula raccomandazioni su come migliorare tale funzionamento, ove opportuno». Si vedano altresì i parr. 6, 7, 8 e 9 dell'art. 21 che prevedono rispettivamente: a) la possibilità per gli Stati membri di istituire organismi di risoluzione extragiudiziale delle controversie o di sostenere l'attività di quelli che hanno certificato; b) la possibilità di revocare la certificazione ove vengano meno le condizioni di cui al par. 3, assicurando un contradditorio preventivo prima di dar corso alla decisione; c) l'obbligo per il coordinatore dei servizi digitali di comunicare alla Commissione gli organismi certificati; d) il fatto che l'art. 21 lasci «impregiudicati la direttiva 2013/11/UE e le procedure e gli organismi di risoluzione alternativa delle controversie per i consumatori istituiti a norma di tale direttiva».

[39] Il par. 5 dell'art. 21 prevede altresì che prima «di avviare la risoluzione delle controversie, gli organismi di risoluzione extragiudiziale delle controversie certificati comunicano al destinatario del servizio, ivi compresi le persone o gli enti che hanno presentato una segnalazione, e al fornitore della piattaforma online interessata i diritti o i meccanismi utilizzati per determinarli».

[40] Che si rifanno alla logica delle *alternative dispute resolution* (ADR).

specie lì dove il sistema di reclamo interno alla piattaforma online non abbia dato gli esiti sperati o comunque presenti criticità, senza dover necessariamente adire l'autorità giudiziaria o in generale gli attori pubblici di *enforcement* e senza che l'innesco di tale binario alternativo di risoluzione delle controversia pregiudichi il diritto di poter percorrere comunque, in qualsiasi fase, le "strade" della giurisdizione statale.
Ciò potrà comportare benefici anche per gli stessi operatori digitali e, soprattutto, per la gestione statale dei servizi giudiziari, nella misura in cui tali ADR, se correttamente implementate, possono aiutare gli Stati a raggiungere l'obiettivo di gestire in modo più efficiente la macchina della giustizia, non aumentando la mole (in molti Paesi già considerevole) dei contenziosi[41].

3.3. Le previsioni in tema di segnalatori attendibili

L'art. 22 del DSA prevede l'obbligo per le piattaforme online di adottare «le misure tecniche e organizzative necessarie» per trattare con priorità e decidere «senza indebito ritardo» le segnalazioni circa la presenza di contenuti illegali presentate, tramite il meccanismo di *notice and action* di cui all'art. 16, da «segnalatori attendibili» entro «il loro ambito di competenza designato».
In particolare, la qualifica di segnalatore attendibile viene riconosciuta, a richiesta di qualunque ente, dal coordinatore dei servizi digitali «dello Stato membro in cui è stabilito il richiedente», a condizione che quest'ultimo dimostri di soddisfare una serie di condizioni specificamente indicate dal par. 2 dell'art. 22 e tese a garantire, tra l'altro, l'indipendenza, la particolare *expertise* e la diligenza di tali *trusted flaggers*[42], i quali, tra l'altro, devono pubblicare relazioni almeno annuali sulle loro attività[43] e possono ve-

[41] Per un commento a queste previsioni del DSA in tema di risoluzione alternativa delle controversie, nonché per una disamina del loro impatto sulla nostra legislazione nazionale in tema di ADR, v. G. Gioia - A. Bigi, *La risoluzione stragiudiziale delle controversie nel mercato dei servizi digitali (artt. 17, 20, 21, 24, 35 – Capo III, Sezioni 2, 3 e 5)*, in *Diritto di internet*, 1, 2023, 39 ss. V. altresì A.M. Felicetti, *La risoluzione extragiudiziale delle dispute nei mercati digitali: alcune novità dall'Europa*, in *Rivista trimestrale di diritto e procedura civile*, 1, 2023, 197 ss.

[42] In particolare, il par. 2 dell'art. 22 del DSA stabilisce che «La qualifica di «segnalatore attendibile» a norma del presente regolamento viene riconosciuta, su richiesta di qualunque ente, dal coordinatore dei servizi digitali dello Stato membro in cui è stabilito il richiedente al richiedente che abbia dimostrato di soddisfare tutte le condizioni seguenti: a) dispone di capacità e competenze particolari ai fini dell'individuazione, dell'identificazione e della notifica di contenuti illegali; b) è indipendente da qualsiasi fornitore di piattaforme online; c) svolge le proprie attività al fine di presentare le segnalazioni in modo diligente, accurato e obiettivo».

[43] Il par. 3 dell'art. 22 del DSA prevede specificamente che «I segnalatori attendibili pubblicano, almeno una volta all'anno, relazioni facilmente comprensibili e dettagliate sulle segnalazioni presentate conformemente all'articolo 16 durante il periodo di riferimento. La relazione elenca almeno il numero di segnalazioni classificate in base: a) all'identità del prestatore di servizi di memorizzazione di informazioni; b) al tipo di presunto contenuto illegale notificato; c) alle azioni adottate dal prestatore. Tali relazioni includono una spiegazione delle procedure in atto per assicurare che il segnalatore attendibile mantenga la propria indipendenza. I segnalatori attendibili inviano tali relazioni al coordinatore dei servizi digitali che ha conferito la qualifica e le mettono a disposizione del pubblico. Le informazioni in tali relazioni non contengono dati personali». Inoltre, ai sensi dei parr. 4, 5 e 8 dell'art. 22 in commento i coordinatori dei servizi digitali devono comunicare alla Commissione – la quale predisporrà una banca dati accessibile al pubblico con l'elenco di tutti i segnalatori attendibili e potrà emanare, se necessario, «orientamenti

dersi revocata la qualifica di segnalatori attendibili, anche su istanza delle piattaforme online, ove abbiano presentato un numero significativo di segnalazioni infondate o, comunque, in generale, ove siano venute meno le condizioni stabilite dal paragrafo 2[44].
Il considerando 61 del DSA fornisce interessanti chiarimenti circa le particolari figure cui il decisore pubblico europeo ha evidentemente pensato nel costruire tale disposizione, specificando che può trattarsi sia di enti di natura pubblica (ad es. Europol o le unità addette alle segnalazioni di contenuti terroristici su internet) sia di organismi privati (ad es. gli enti facenti parte della «rete di linee di emergenza per la segnalazione di materiale pedopornografico INHOPE e le organizzazioni impegnate nella notifica dei contenuti razzisti e xenofobi illegali online»), indicando tra l'altro l'importanza, per «evitare di attenuare il valore aggiunto di tale meccanismo», di «limitare il numero complessivo di qualifiche» conferite in conformità al DSA.
La decisione del legislatore eurounitario, in definitiva, è quella di obbligare le piattaforme online a predisporre una sorta di canale di segnalazione privilegiato per tali enti, nella convinzione che questi possano supportare in modo particolarmente efficace questi operatori digitali nelle loro attività di "*digital patrolling*", secondo un approccio improntato alla cooperazione tra i vari *stakeholder* che, come noto, ha rivestito e riveste grande importanza nella lotta alle campagne (coordinate e non) di disinformazione[45].

per assistere i fornitori di piattaforme online e i coordinatori dei servizi digitali nell'applicazione dei paragrafi 2, 6 e 7» – ogni provvedimento relativo al riconoscimento o alla sospensione/revoca della qualifica di segnatore attendibile.

[44] I parr. 6 e 7 dell'art. 22 del DSA, invero, sanciscono che «6. Se un fornitore di piattaforme online dispone di informazioni indicanti che un segnalatore attendibile ha presentato un numero significativo di segnalazioni non sufficientemente precise, inesatte o non adeguatamente motivate avvalendosi dei meccanismi di cui all'articolo 16, comprese le informazioni raccolte in relazione al trattamento dei reclami tramite i sistemi interni di gestione dei reclami di cui all'articolo 20, paragrafo 4, comunica dette informazioni al coordinatore dei servizi digitali che ha riconosciuto la qualifica di segnalatore attendibile all'ente interessato, fornendo le spiegazioni e i documenti giustificativi necessari. Una volta ricevute le informazioni dal fornitore delle piattaforme online e ove il coordinatore dei servizi digitali ritenga che vi siano motivi legittimi per avviare un'indagine, la qualifica di segnalatore attendibile è sospesa durante il periodo dell'indagine. Tale indagine è condotta senza indebiti ritardi. 7. Il coordinatore dei servizi digitali che ha riconosciuto la qualifica di segnalatore attendibile a un ente revoca tale qualifica se accerta, a seguito di un'indagine avviata di propria iniziativa o in base a informazioni ricevute da terzi, comprese le informazioni fornite da un fornitore di piattaforme online a norma del paragrafo 6, che l'ente non soddisfa più le condizioni di cui al paragrafo 2. Prima di revocare tale qualifica, il coordinatore dei servizi digitali dà all'ente in questione la possibilità di rispondere alle constatazioni della sua indagine e di reagire alla sua intenzione di revocarne la qualifica di segnalatore attendibile».

[45] Per una panoramica dei vari approcci in materia di contrasto alla disinformazione v. O. Pollicino, *The European approach to disinformation: comparing supranational and national measures*, in *Annuario di diritto comparato e di studi legislativi*, 1, 2020, 175 ss. In generale, sulle dinamiche di co-regolazione pubblico-privato che riguardano le piattaforme v. ampiamente A. Simoncini, *La co-regolazione delle piattaforme digitali*, in *Rivista trimestrale di diritto pubblico*, 4, 2022, 1031 ss.

4. Gli obblighi supplementari a carico delle *Very Large Online Platforms (VLOPs)* e dei *Very Large Online Search Engines (VLOSEs)*: la scommessa del legislatore europeo sulla compliance

La sezione V del Capo III del DSA corrisponde al "gradino" più elevato del sistema di *due diligence obligation* a livelli di intensità crescente costruito dal nuovo regolamento europeo, rivolgendosi ai motori di ricerca e alle piattaforme online di "dimensioni molto grandi", qualificandosi in questo modo gli operatori che vengono espressamente designati come tali da una decisione della Commissione europea[46], a norma dell'art. 33 DSA, con riferimento a coloro «che hanno un numero medio mensile di destinatari attivi[47] del servizio nell'Unione pari o superiore a 45 milioni».

Si tratta, per così dire, dei *target* più importanti della strategia di regolazione del legislatore eurounitario, rispetto ai quali il DSA riserva incisivi poteri di *enforcement* (esercitati direttamente, tra l'altro, avuto riguardo a tale sezione del regolamento, dalla Commissione europea, così da "contrapporre" un interlocutore sovranazionale "di peso" a società, esse stesse, multinazionali e detentrici di rilevanti poteri[48]), nonché i più significativi obblighi di conformità che si aggiungono, come sappiamo, a quelli delle sezioni del regolamento precedentemente analizzate.

Tra tali operatori, del resto, si collocano i più importanti *social network* (tra gli altri, Facebook e Twitter, in base alla prima *designation decision* resa pubblica dalla Commissione)[49]

---

[46] L'art. 24 del DSA impone invero alle piattaforme online e ai motori di ricerca di pubblicare nella loro interfaccia online e comunicare al coordinatore dei servizi digitali del luogo di stabilimento e alla Commissione, su loro richiesta, le informazioni sul numero medio mensile di destinatari attivi del servizio, calcolato in conformità alle metodologie stabilite con atti delegati dalla Commissione stessa, fermo restando che, ai sensi dell'art. 33, la Commissione può comunque adottare la decisione circa la designazione di tali operatori come piattaforme o motori di ricerca 'di dimensioni molto grandi' sulla base di «qualsiasi altra informazione a sua disposizione», dovendo tuttavia in quest'ultimo caso garantire al *provider* una sorta di contradditorio preventivo, dandogli la possibilità di presentare il proprio parere in merito a tale decisione entro dieci giorni lavorativi. Si prevede, inoltre, che la Commissione adotti tali decisioni «previa consultazione dello Stato membro di stabilimento o tenuto conto delle informazioni fornite dal coordinatore dei servizi digitali del luogo di stabilimento a norma dell'articolo 24, paragrafo 4». La Commissione, infine, deve pubblicare sulla Gazzetta Ufficiale dell'Unione europea, e costantemente aggiornare, l'elenco degli operatori qualificati 'di dimensioni molto grandi', potendo porre fine alla designazione del *provider* come tale ove successivamente quest'ultimo non soddisfi più tale requisito quantitativo.

[47] L'art. 3 del DSA fornisce, alle lett. p) e q), le seguenti definizioni: «p) «destinatario attivo di una piattaforma online»: il destinatario del servizio che si è avvalso di una piattaforma online richiedendo alla piattaforma online di ospitare informazioni o esponendosi alle informazioni ospitate dalla piattaforma online e diffuse attraverso la sua interfaccia online; q) «destinatario attivo di un motore di ricerca online»: il destinatario del servizio che ha formulato una richiesta a un motore di ricerca online e si è esposto a informazioni indicizzate e presentate sulla sua interfaccia online».

[48] Cfr. nel dettaglio, anche per ogni ulteriore riferimento, il tezo saggio della presente sezione (di R. Sabia, *L'*enforcement *pubblico del* Digital Services Act *tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni*). Che si tratti degli interlocutori più importanti in qualche misura è "dimostrato" anche dal fatto che ai sensi dell'art. 43 DSA la Commissione europea «addebita ai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi un contributo annuale per le attività di vigilanza al momento della loro designazione a norma dell'articolo 33».

[49] In conformità al DSA, il 25 aprile 2023 la Commissione ha già provveduto a designare come di "dimensioni molto grandi" 2 motori di ricerca (Bing e Google Search) e 17 piattaforme (Alibaba

che, nel contrasto alla disinformazione, esercitano un ruolo assolutamente decisivo e che devono essere necessariamente chiamati dal decisore pubblico a svolgere un ruolo proattivo, come abbiamo cercato di argomentare già nei precedenti cicli della ricerca[50]. Ed è proprio quest'ultimo obiettivo quello che il DSA tenta qui di raggiungere, tramite una scelta di *policy* ben precisa: quella di puntare sugli stilemi, sui paradigmi, sugli strumentari ormai classici dell'era della *corporate compliance*, già sperimentati in qualche misura in altri regolamenti europei (spicca su tutti ovviamente, per importanza e contiguità con il DSA, il *General Data Protection Regulation*)[51].

Come subito vedremo, peraltro, il legislatore eurounitario sembra scommettere su tale scelta di politica del diritto in modo ancor più deciso, disciplinando con un particolare livello di dettaglio, per quanto qui interessa, i criteri di valutazione e gestione dei rischi, l'architettura dei sistemi e delle metodologie di controllo interno, i meccanismi di cooperazione pubblico-privato specie nella risposta alle crisi.

Si entra qui, insomma, nel "cuore pulsante" del regolamento, che ha a che fare con la gestione e la mitigazione dei "*systemic risks*" degli ambienti digitali moderni – per ciò che concerne, tra l'altro, i diritti fondamentali, la libertà di espressione, il pluralismo dei media, i diritti dei minori, l'integrità dei processi elettorali, la salute e la sicurezza pubblica – la cui valutazione e mitigazione viene affidata agli stessi operatori che generano simili rischi e alle dinamiche di cooperazione istituzionalizzata tra pubblico-privato, secondo modelli di regolazione, appunto, ormai consolidati in vari ordinamenti e in diversi settori di disciplina (si pensi all'ambiente, alla sicurezza sul lavoro, alla *privacy*)[52].

4.1. Obblighi di *risk assessment*

La prima *due diligence obligation* aggiuntiva per i detti operatori di "dimensioni molto grandi" riguarda l'obbligo di effettuare almeno una volta all'anno, nonché «in ogni caso prima dell'introduzione di funzionalità che possono avere un impatto critico», un *assessment* concernente l'individuazione, l'analisi e la valutazione «con diligenza» degli eventuali «rischi sistemici» derivanti dalla progettazione, dal funzionamento o dall'uso dei loro servizi e dei relativi sistemi (anche algoritmici).

L'art. 34 del DSA esige un'analisi specifica «e proporzionata ai rischi sistemici, tenendo in considerazione la loro gravità e la loro probabilità», che comprenda i seguenti "*systemic risks*": *a)* la diffusione di contenuti illegali tramite il proprio servizio; *b)* «eventuali effetti negativi, attuali o prevedibili» collegati alla propria attività e relativi all'esercizio di diritti fondamentali tra cui, tra l'altro, la tutela dei dati personali, la libertà di espres-

AliExpress; Amazon Store; Apple AppStore; Booking.com; Facebook; Google Play; Google Maps; Google Shopping; Instagram; LinkedIn; Pinterest; Snapchat; TikTok; Twitter; Wikipedia; YouTube; Zalando): cfr. *europa.eu/commission*.

[50] V. *supra* par. 1 per tutti i necessari rinvii. In argomento v. anche, da ultimo, le considerazioni di V. Zeno-Zencovich, *The EU regulation of speech. A critical view*, in questa *Rivista*, 1, 2023, 14.

[51] Da ultimo, per un confronto tra DSA e GDPR, v., anche per ogni ulteriore approfondimento, M. Iaselli, Digital Services Act *e* Privacy, in *Diritto di internet*, 1, 2023, 67 ss.

[52] V., per tutti, A. Gullo, voce *Compliance*, in G. Mannozzi - C. Perini - F. Consulich - C. Piergallini - M. Scoletta - C. Sotis (a cura di), *Studi in onore di Carlo Enrico Paliero*, Milano, 2022, 1289 ss.

sione e di informazione, inclusi il pluralismo dei media, la non discriminazione, i diritti del minore, la tutela dei consumatori[53]; *c)* eventuali effetti negativi «sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica»; *d)* qualsiasi incidenza non positiva 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».
Si tratta, a ben vedere, non solo dei principali ambiti rispetto ai quali diversi *social media* già disciplinano *policy* interne più o meno articolate[54], ma anche di alcuni degli interessi sui quali la *misinformation* e le azioni (coordinate e non) di disinformazione possono più significativamente incidere, con la conseguenza che inevitabilmente piattaforme online e motori di ricerca "*very large*" saranno chiamati, secondo la predetta cadenza periodica, ad autovalutare attentamente il rischio che simili comportamenti possano essere compiuti nell'ambito dei propri servizi e, come vedremo tra poco[55], a farsi carico del delicato compito di introdurre misure per mitigare questi potenziali effetti negativi. Lo stesso considerando 84 del DSA, del resto, chiarisce come tali fornitori dovrebbero «prestare particolare attenzione al modo in cui i loro servizi sono utilizzati per diffondere o amplificare contenuti fuorvianti o ingannevoli, compresa la disinformazione».
Molto opportunamente, poi, il par. 2 dell'art. 34 del DSA detta ulteriori criteri per "guidare" e orientare correttamente tale *risk assessment*, nella misura in cui si esige che la valutazione in questione tenga conto «in particolare, dell'eventualità e del modo in cui i seguenti fattori influenzano uno dei rischi sistemici di cui al paragrafo 1: a) la progettazione dei loro sistemi di raccomandazione e di qualsiasi altro sistema algoritmico pertinente; b) i loro sistemi di moderazione dei contenuti; c) le condizioni generali applicabili e la loro applicazione; d) i sistemi di selezione e presentazione delle pubblicità; e) le pratiche del fornitore relative ai dati […]; [la] manipolazione intenzionale del loro servizio, anche mediante l'uso non autentico o lo sfruttamento automatizzato del servizio, nonché l'amplificazione e la diffusione potenzialmente rapida e ampia di contenuti illegali e di informazioni incompatibili con le condizioni generali»[56].
La centralità di questi aspetti, nel contrasto alla disinformazione, è di palmare evidenza. Anche nel corso dei precedenti cicli della ricerca[57], infatti, avevamo osservato come

[53] Nel dettaglio, l'art. 34, par. 1, lett. b) del DSA si riferisce a «eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali, in particolare i diritti fondamentali alla dignità umana sancito nell'articolo 1 della Carta, al rispetto della vita privata e familiare sancito nell'articolo 7 della Carta, alla tutela dei dati personali sancito nell'articolo 8 della Carta, alla libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, sanciti nell'articolo 11 della Carta, e alla non discriminazione sancito nell'articolo 21 della Carta, al rispetto dei diritti del minore sancito nell'articolo 24 della Carta, così come all'elevata tutela dei consumatori, sancito nell'articolo 38 della Carta».

[54] Abbiamo effettuato un'analisi di dettaglio di queste politiche in E. Birritteri, *Punire la disinformazione*, cit., 304 ss.

[55] Cfr. il paragrafo successivo.

[56] Si prevede altresì che «La valutazione tiene conto di specifici aspetti regionali o linguistici, anche laddove siano specifici di uno Stato membro. 3 I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi conservano i documenti giustificativi delle valutazioni dei rischi per almeno tre anni dopo l'esecuzione delle valutazioni dei rischi e, su richiesta, li comunicano alla Commissione e al coordinatore dei servizi digitali del luogo di stabilimento».

[57] Cfr. *supra*, par. 1, per tutti i necessari rinvii rispetto ai temi qui di seguito menzionati. Ampiamente su tali profili v. recentemente A. Manganelli - A. Nicita, *Regulating Digital Markets. The European Approach*, Cham, 2022, 177 ss.

alcune caratteristiche specifiche del modello di business di tali *Big Tech* siano in grado di favorire la diffusione dei possibili effetti negativi che la condivisione di notizie false online può generare su interessi come l'integrità dei processi e delle consultazioni elettorali, la salute pubblica (si pensi alle molte informazioni false condivise in relazione al Covid-19), il pluralismo dei media. Ad esempio, come noto, i sistemi di raccomandazione tendono a riproporre all'utente contenuti sempre più in linea con la propria precedente attività in rete, con la conseguenza di innescare un continuo "bombardamento" nei suoi riguardi di contenuti falsi che lo hanno già in precedenza interessato – e che rischiano così di divenire rapidamente virali in rete con tutto ciò che di negativo può derivarne – o di *post* potenzialmente molto pericolosi per il suo benessere psicofisico (si pensi a utenti che tendono ad essere attratti, per uno stato depressivo, da informazioni relative ad atti di autolesionismo). Si può far riferimento, altresì, alle tecniche di manipolazione intenzionale del servizio (tra cui l'interazione artificiosa tra più *account* per aumentare in modo fraudolento la visibilità di certe notizie, o l'uso agli stessi fini di *bot* automatici e profili *fake*) spesso utilizzati in campagne coordinate di disinformazione. Ancora, palese è il richiamo, nel riferimento da parte dell'art. 34 del DSA alle modalità di moderazione dei contenuti e alla definizione delle condizioni generali d'uso del servizio, al rischio che una non equilibrata politica di articolazione di simili *policy* interne finisca per risolversi in una illegittima censura nell'ambito del libero confronto politico, e, in generale, in una forma di illecita interferenza sulla libertà di espressione di personaggi pubblici e cittadini.

Di qui l'impatto di tali realtà digitali sui menzionati diritti fondamentali e la necessità per le organizzazioni in questione di autovalutare con attenzione tali risvolti potenzialmente "perversi" dei loro sistemi e servizi.

Si tratta di una norma chiave che si pone l'obiettivo di sensibilizzare le piattaforme sull'esigenza di farsi carico degli interessi di tutti gli *stakeholder* che possono in qualche misura essere influenzati dalla loro attività, non potendo le esigenze di *business* e di profitto essere perseguite a discapito di tali diritti individuali e beni collettivi[58]. Ciò secondo un approccio sistematico e sfruttando la capacità organizzativa e di gestione di modelli di *compliance* e metodologie di analisi del rischio che simili grandi *corporation* certamente possiedono[59].

Sotto tale profilo, allora, ci pare che questa disposizione detti una condivisibile cornice pubblicistica di riferimento per una attività di *risk assessment* che appare oggi indispensabile e che, pur ponendo un significativo onere organizzativo e gestionale in capo a tali attori, sembra proporzionata alla loro "potenza di fuoco" sul mercato globale e un bilanciamento tutto sommato più che ragionevole tra i vari interessi contrapposti[60].

[58] Su tale esigenza con specifico riguardo alla lotta alla disinformazione v. ampiamente P. Severino, voce *Disinformazione*, in G. Mannozzi - C. Perini - F. Consulich - C. Piergallini - M. Scoletta - C. Sotis (a cura di), *Studi in onore di Carlo Enrico Paliero*, Milano, 2022, 1373 ss.

[59] In generale, sul tema dell'articolazione della *compliance* nelle realtà multinazionali, v. da ultimo in dettaglio S. Manacorda, *The "Dilemma" of Criminal Compliance for Multinational Enterprises in a Fragmented Legal Word*, in S. Manacorda - F. Centonze (a cura di), *Corporate Compliance on a Global Scale*, Cham, 2022, 67 ss. Sul punto v. anche V. Mongillo, *Presente e futuro della* compliance *penale*, in *sistema penale.it*, 11 gennaio 2022.

[60] In generale, sull'approccio del DSA in punto di bilanciamento tra i vari interessi contrapposti, v. G.

L'auspicio dei regolatori, tra l'altro, è che la possibilità per i soggetti regolati di essere esposti, in caso di non conformità con tali obblighi di *due diligence*, a sanzioni e meccanismi di *enforcement* potenzialmente molto efficaci[61], certamente stimolerà le c.d. VLOPs (*Very Large Online Platforms*) e i c.d. VLOSEs (*Very Large Online Search Engines*) ad effettuare tali valutazioni con serietà e significativo impegno, scongiurando la possibilità di legittimare forme di c.d. mera *cosmetic* o *paper compliance*[62].

4.2. Le previsioni in punto di mitigazione dei rischi

Il DSA disciplina naturalmente anche la fase conseguente al *risk assessment* effettuato ai sensi dell'art. 34, richiedendo alle piattaforme online e ai motori di ricerca di dimensioni molto grandi l'adozione di «misure di attenuazione ragionevoli, proporzionate ed efficaci, adattate ai rischi sistemici specifici individuati a norma dell'articolo 34, prestando particolare attenzione agli effetti di tali misure sui diritti fondamentali».
L'art. 35 contempla un elenco molto fitto di alcune possibili "*mitigation measures*", strettamente interconnesse agli ambiti di rischio identificati dall'art. 34, tra cui: l'adeguamento di progettazione, caratteristiche e funzionamento dei servizi, condizioni generali e correlato *enforcement*, sistemi algoritmici, di raccomandazione e pubblicità, interfacce online; misure di sensibilizzazione e l'adeguamento «delle procedure di moderazione dei contenuti, compresa la velocità e la qualità del trattamento delle segnalazioni concernenti tipi specifici di contenuti illegali e, se del caso, la rapida rimozione dei contenuti oggetto della notifica o la disabilitazione dell'accesso agli stessi, in particolare in relazione all'incitamento illegale all'odio e alla violenza online, nonché l'adeguamento di tutti i processi decisionali pertinenti e delle risorse dedicate alla moderazione dei contenuti»[63]; l'avvio o l'adeguamento della cooperazione con i *trusted flaggers* e l'attuazione delle decisioni degli organismi di risoluzione extragiudiziale delle controversie; la cooperazione con altre piattaforme o motori di ricerca sulla base di codici di condotta e protocolli di crisi *ex* art. 45 e 48 del DSA; misure a tutela dei minori come «strumenti di verifica dell'età e di controllo parentale, o strumenti volti ad aiutare i minori a segnalare abusi o ottenere sostegno»; misure specifiche afferenti, in sostanza, al fenomeno dei cc.dd. *deep fake*[64].

Caggiano, *La proposta di* Digital Services Act *per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in *Annali AISDUE*, 1, 2021, 28.

[61] Cfr. ancora il terzo saggio della presente sezione monografica.

[62] Su tale nozione v., per tutti, V. Mongillo, *La responsabilità penale tra individuo ed ente collettivo*, Torino, 2018, 187 e 471.

[63] La lett. f) del par. 1 dell'art. 35 del DSA menziona anche, in generale, «il rafforzamento dei processi interni, delle risorse, della sperimentazione, della documentazione o della vigilanza sulle loro attività, in particolare per quanto riguarda il rilevamento dei rischi sistemici».

[64] In particolare, ai sensi dell'art. 35, par. 1, lett. k) del DSA, si tratta del «il ricorso a un contrassegno ben visibile per fare in modo che un elemento di un'informazione, sia esso un'immagine, un contenuto audio o video, generati o manipolati, che assomigli notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che a una persona appaia falsamente autentico o veritiero, sia distinguibile quando è presentato sulle loro interfacce online e, inoltre, la fornitura di una funzionalità di facile utilizzo che consenta ai destinatari del servizio di indicare tale informazione». Per un recente approfondimento del

Al di là di alcune indicazioni di maggiore dettaglio (ad es. in tema di azioni a tutela dei minori e di contrasto, come visto da ultimo, ai *deep fake*), quindi, il DSA menziona soltanto, per così dire, le macro-tipologie di misure che le piattaforme possono autonormare e adottare al fine di gestire e mitigare i rischi connessi all'impatto dei loro servizi sui detti diritti fondamentali e interessi individuali e collettivi. Ci si riferisce, insomma, all'adeguamento di certe *policy* o determinati processi, ma non si forniscono indicazioni più precise e puntuali su *come farlo*, sulle specifiche misure adottabili per conseguire l'obiettivo di risolvere le criticità delle procedure individuate in sede di valutazione del rischio. Il regolatore europeo, in linea con quanto si è visto accade anche rispetto ad altre disposizioni del regolamento, è sempre ben attento a non imporre agli operatori digitali particolari e dettagliate politiche sull'organizzazione e la gestione operativa dei loro servizi, lasciando loro, anche in tale sede, un ampio margine di apprezzamento.
La convinzione pare essere quella dell'impossibilità o comunque dell'inopportunità di fornire procedure e modelli di gestione "preconfezionati", positivizzando analiticamente le cautele imposte, e della necessità, piuttosto, di lasciare liberi i soggetti regolati di costruire autonomamente le proprie "regole interne" secondo una logica *taylor made*, fornendo indicazioni di scopo di carattere generale e qui, in qualche misura, anche una metodologia di analisi e un elenco di possibili contromisure e ambiti di rischio specifici da considerare, menzionando soltanto il *genus* di riferimento delle varie possibili "*effective mitigation measures*"[65].
La scelta finale e "di merito" circa le *policy* da adottare in concreto, quindi, spetterà sempre agli operatori, il che ci pare sia un tema molto significativo anche sul versante sanzionatorio, nella misura in cui il DSA, in tale ambito, potrà a rigore dirsi violato allorquando i soggetti regolati abbiamo in tutto o in parte omesso o non effettuato correttamente[66], secondo i predetti generali criteri metodologici di analisi e gestione, lo svolgimento delle attività di *risk assessment* e *management*, e non già, di per sé, per la (motivata) scelta di non adottare (o di adottare in un certo modo) le specifiche, singole misure di gestione del rischio, rispetto alla quale le *corporation* mantengono un autonomo potere decisorio; nell'introdurre l'elenco delle tipologie di politiche di mitigazione

tema cfr. M. Cazzaniga, *Una nuova tecnica (anche) per veicolare disinformazione: le risposte europee ai* deepfakes, in questa *Rivista*, 1, 2023, 170 ss.

[65] La dottrina ha quindi evidenziato come il DSA, in tal senso, adotti un approccio in qualche misura riportabile al concetto di *meta-regulation* o *enforced-self regulation*: v. N. Zingales, *The DSA as a Paradigm Shift for Online Intermediaries' Due Diligence*, in J. van Hoboke - J.P. Quintais - N. Appelman - R. Fahy - I. Buri - M. Straub (a cura di), *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implications*, Berlino, 2023, 213-214, il quale, da un lato, evidenzia che «*This approach, which on the one hand leaves businesses with a significant amount of discretion in the implementation of regulatory principles, and on the other involves a process of continuous evaluation and monitoring of the results, has been called "metaregulation" or "enforced self-regulation": "meta" because one (macro) regulator oversees another (micro) regulator in their management of risk; "enforced" because, in case of inadequacy of the self-regulatory practices, the (macro) regulator has the power to take enforcement measures», e, dall'altro lato, che «while the shift to a metaregulatory model should be welcomed for enabling reflexive and adaptive regulation, we must also be weary of its risk of collapsing in the absence of well-resourced and independent institutions*». Per un inquadramento approfondito del fenomeno dell'autonormazione (e delle varie classificazioni operabili) in relazione al sistema penale v. la recente indagine monografica di D. Bianchi, *Autonormazione e diritto penale. Intersezioni, potenzialità, criticità*, Torino, 2022.

[66] Ad esempio, effettuando soltanto un'analisi molto vaga, sommaria e superficiale dei rischi legati, in generale, a un certo *business* digitale, senza tarare tale *assessment* sulle proprie specificità, sulle proprie concrete dinamiche operative, sui propri servizi, nella logica di una valutazione realmente *tailor made*.

dei rischi suggerite alle piattaforme, invero, il testo originale in inglese del DSA utilizza la chiara dicitura per cui «such measures *may*[67] include» (cioè possono, non devono).
Ai sensi dei parr. 2 e 3 dell'art. 35, ad ogni modo, le istituzioni europee potranno adottare periodicamente relazioni e orientamenti volti ad agevolare, secondo dinamiche flessibili e tali da assicurare anche consultazioni pubbliche con un coinvolgimento preventivo dei vari *stakeholder*, la diffusione delle *best practice* implementate nel settore e informazioni di rilievo circa i rischi sistemici più rilevanti, così da aiutare concretamente le piattaforme online e i motori di ricerca ad adeguarsi a tali obblighi di *compliance*, fornendo loro indicazioni ancor più puntuali sulle migliori strategie da attuare per conseguire gli obiettivi di prevenzione fissati dal regolamento[68].
L'auspicio, dunque, è che tale interazione tra disciplina normativa e orientamenti integrativi fornite dalle autorità di *enforcement*, che sembra in qualche misura ispirarsi a pratiche ampiamente sperimentate in molti ordinamenti specie con riferimento alla *corporate criminal liability*[69], possa delineare chiaramente le regole del gioco, alla luce del non facile compito qui assegnato dal DSA alle organizzazioni più importanti del mondo digitale. Specie nel settore del contrasto alla disinformazione, del resto, la costruzione e l'im-

[67] Corsivo nostro.

[68] In particolare, si prevede che «2. Il comitato, in cooperazione con la Commissione, pubblica relazioni annuali esaustive. Le relazioni comprendono gli elementi seguenti: a) individuazione e valutazione dei rischi sistemici più rilevanti e ricorrenti segnalati dai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi o identificati mediante altre fonti di informazione, in particolare le informazioni fornite in conformità degli articoli 39, 40 e 42; b) le migliori pratiche che consentano ai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi di attenuare i rischi sistemici individuati. Tali relazioni presentano i rischi sistemici suddivisi per Stato membro in cui si sono verificati e in tutta l'Unione, se del caso. 3. La Commissione, in cooperazione con i coordinatori dei servizi digitali, può emanare orientamenti sull'applicazione del paragrafo 1 in relazione a rischi concreti, con l'obiettivo specifico di presentare le migliori pratiche e raccomandare eventuali misure, tenendo debitamente conto delle possibili conseguenze di tali misure sui diritti fondamentali di tutte le parti interessate sanciti dalla Carta. Nell'elaborazione di tali orientamenti la Commissione organizza consultazioni pubbliche». Inoltre, ai sensi dell'art. 44 del DSA «1. La Commissione consulta il comitato e sostiene e promuove lo sviluppo e l'attuazione di norme volontarie fissate dai competenti organismi di normazione europei e internazionali almeno per quanto riguarda: a) la presentazione elettronica delle segnalazioni di cui all'articolo 16; b) modelli, progettazione e norme di processo per comunicare con i destinatari del servizio in modo facilmente fruibile sulle restrizioni derivanti dalle condizioni generali e sulle relative modifiche; c) la presentazione elettronica di segnalazioni da parte dei segnalatori attendibili a norma dell'articolo 22, anche per mezzo di interfacce di programmazione delle applicazioni; d) interfacce specifiche, comprese le interfacce di programmazione delle applicazioni, per agevolare il rispetto degli obblighi di cui agli articoli 39 e 40; e) le revisioni delle piattaforme online di dimensioni molto grandi e dei motori di ricerca online di dimensioni molto grandi a norma dell'articolo 37; f) l'interoperabilità dei registri della pubblicità di cui all'articolo 39, paragrafo 2; g) la trasmissione di dati tra intermediari pubblicitari a sostegno degli obblighi di trasparenza a norma dell'articolo 26, paragrafo 1, lettere b), c) e d); h) misure tecniche che consentano il rispetto degli obblighi in materia di pubblicità di cui al presente regolamento, compresi gli obblighi riguardanti i contrassegni ben visibili per la pubblicità e le comunicazioni commerciali di cui all'articolo 26; i) interfacce di scelta e presentazione delle informazioni sui principali parametri dei diversi tipi di sistemi di raccomandazione, conformemente agli articoli 27 e 38; j) norme per misure mirate a tutela dei minori online. 2. La Commissione sostiene l'aggiornamento delle norme alla luce degli sviluppi tecnologici e del comportamento dei destinatari dei servizi in questione. Le informazioni pertinenti relative all'aggiornamento delle norme devono essere disponibili al pubblico e facilmente accessibili».

[69] V. da ultimo l'approfondita indagine monografica di R. Sabia, *Responsabilità da reato degli enti e paradigmi di validazione dei modelli organizzativi. Esperienze comparate e scenari di riforma*, Torino, 2022.

plementazione di *policy* da parte delle piattaforme presuppone una complessa opera di bilanciamento tra diritti fondamentali individuali e collettivi tra loro contrapposti, per cui occorre che quella alle *Big Tech* private non sia una delega totalmente "in bianco", ma, al contrario, sia frutto di una strategia di gestione condivisa di tali rischi[70], sotto la guida dei decisori pubblici, anche e soprattutto alla luce dei rilevanti poteri sanzionatori che possono essere azionati in caso di omesso o non corretto adeguamento a tali obblighi di *due diligence* da parte di questi soggetti economici.

4.3. Il *crisis response mechanism*

L'art. 36 del DSA disciplina una procedura particolare destinata ad applicarsi, con riferimento a piattaforme online e motori di ricerca di dimensioni molto grandi, in condizioni di crisi definite espressamente come «circostanze eccezionali [che] comportano una grave minaccia per la sicurezza pubblica o la salute pubblica nell'Unione o in parti significative di essa». Il considerando 91 del regolamento fornisce, peraltro, alcuni esempi significativi, specificando che tali «crisi potrebbero derivare da conflitti armati o atti di terrorismo, compresi conflitti o atti di terrorismo emergenti, catastrofi naturali quali terremoti e uragani, nonché pandemie e altre gravi minacce per la salute pubblica a carattere transfrontaliero».

Si tratta, a ben vedere, di ambiti particolarmente sensibili proprio rispetto al contrasto alle campagne (coordinate e non) di disinformazione; in numerosissimi casi, infatti, le notizie false maggiormente virali circolate in rete, e tali da poter influire negativamente sui diritti collettivi e individuali in gioco (salute e sicurezza pubblica), hanno avuto ad oggetto proprio le crisi internazionali in questione[71]. Appare quindi chiaro, e di interesse per questa ricerca, il retroterra "socio-criminologico" di riferimento di tale previsione.

Ora, in queste situazioni, la disposizione in questione del DSA prevede che la Commissione europea, su raccomandazione del comitato europeo per i servizi digitali[72], possa

[70] V. l'introduzione alla presente ricerca di A. Gullo, *Contenuti, scopi e traiettoria della ricerca: le nuove frontiere della* compliance *nel mercato digitale*. Su tali profili, in relazione al DSA e con interessanti riferimenti alle indicazioni della giurisprudenza del Corte suprema federale tedesca, v. A. von Ungern-Sternberg, *Freedom of Speech goes Europe – EU Laws for Online Communication*, in A. von Ungern-Sternberg (a cura di), *Content Regulation in the European Union*, cit., 45; nello stesso volume cfr. anche il contributo di R. Janal, *Impacts of the Digital Services Act on the Facebook "Hate Speech" Decision by the German Federal Court of Justice*, 119 ss.

[71] Si veda da ultimo il caso studio – in corso di pubblicazione sul sito istituzionale del MAECI – del terzo ciclo della presente ricerca (*Narrazioni e strategie di propaganda nelle* community *filorusse*), dedicato proprio alla disamina dei fenomeni di disinformazione legati al recente conflitto armato in Ucraina, cui si rinvia per ogni riferimento. In argomento v. anche L. Ciliberti, Free flow of information – *Il contrasto alla disinformazione in tempi di guerra*, in questa *Rivista*, 2, 2022, 349 ss., e S. Lattanzi, *La lotta alla disinformazione nei rapporti tra Unione e Stati terzi alla luce del conflitto russo-ucraino*, ivi, 3, 2022, 158 ss.

[72] L'art. 61 del DSA stabilisce invero che «1. È istituito un gruppo consultivo indipendente di coordinatori dei servizi digitali per la vigilanza sui prestatori di servizi intermediari denominato «comitato europeo per i servizi digitali» («comitato»). 2. Il comitato fornisce consulenza ai coordinatori dei servizi digitali e alla Commissione conformemente al presente regolamento per conseguire gli obiettivi seguenti: a) contribuire all'applicazione coerente del presente regolamento e alla cooperazione efficace dei coordinatori dei servizi digitali e della Commissione nelle materie disciplinate dal presente regolamento;

adottare una decisione «che impone» a tali operatori di intraprendere una o più tra le seguenti azioni: *a)* una valutazione sull'eventualità e, in caso affermativo, sulla portata e sul modo in cui il funzionamento o l'uso dei propri servizi può, si legge letteralmente, «contribuire» a una delle suindicate minacce gravi per la sicurezza o la salute pubblica; *b)* l'individuazione e l'applicazione di una delle misure di attenuazione dei rischi sistemici pocanzi menzionate e definite dall'art. 35, o dall'art. 48, par. 2, del DSA – si tratta, in quest'ultimo caso, dei protocolli di crisi volontari che possono essere elaborati, sperimentati e applicati, sempre per far fronte a analoghe situazioni emergenziali, tra tali organizzazioni e la Commissione europea[73] –, così da «prevenire, eliminare o limitare tale contributo alla grave minaccia individuata»; *c)* una relazione alla Commissione in merito alle misure adottate e alle valutazioni effettuate nel corso dell'implementazione di tale meccanismo di risposta alla crisi[74].

b) coordinare e contribuire agli orientamenti e all'analisi della Commissione, dei coordinatori dei servizi digitali e di altre autorità competenti sulle questioni emergenti nel mercato interno in relazione alle materie disciplinate dal presente regolamento; c) assistere i coordinatori dei servizi digitali e la Commissione nella vigilanza sulle piattaforme online di dimensioni molto grandi».

[73] L'art. 48 nel dettaglio dispone che «1. Il comitato può raccomandare alla Commissione di avviare l'elaborazione, conformemente ai paragrafi 2, 3 e 4, di protocolli di crisi volontari per affrontare situazioni di crisi. Dette situazioni sono strettamente limitate a circostanze straordinarie che incidono sulla sicurezza pubblica o sulla salute pubblica. 2. La Commissione incoraggia e facilita i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi e, ove opportuno, i fornitori di altre piattaforme online o di altri motori di ricerca online a partecipare all'elaborazione, alla sperimentazione e all'applicazione di tali protocolli di crisi. La Commissione provvede affinché tali protocolli di crisi comprendano una o più delle misure seguenti: a) la ben evidenziata visualizzazione di informazioni sulla situazione di crisi fornite dalle autorità degli Stati membri o a livello di Unione o, a seconda del contesto della crisi, da altri organismi competenti affidabili; b) la garanzia che il fornitore di servizi intermediari designi uno specifico punto di contatto per la gestione delle crisi; ove opportuno, può trattarsi del punto di contatto elettronico di cui all'articolo 11 oppure, nel caso dei fornitori di piattaforme online di dimensioni molto grandi o di motori di ricerca online di dimensioni molto grandi, del responsabile della conformità di cui all'articolo 41; c) ove opportuno, l'adeguamento delle risorse destinate a garantire il rispetto degli obblighi di cui agli articoli 16, 20, 22, 23 e 35 alle esigenze che sorgono dalla situazione di crisi. 3. La Commissione coinvolge, se opportuno, le autorità degli Stati membri e può coinvolgere anche le istituzioni, gli organi e gli organismi dell'Unione nell'elaborazione, nella sperimentazione e nella supervisione dell'applicazione dei protocolli di crisi. Ove necessario e opportuno, la Commissione può coinvolgere anche le organizzazioni della società civile o altre organizzazioni competenti nell'elaborazione dei protocolli di crisi. 4. La Commissione mira a garantire che i protocolli di crisi definiscano chiaramente tutti gli elementi seguenti: a) i parametri specifici per determinare che cosa costituisca la specifica circostanza eccezionale che il protocollo di crisi intende affrontare e gli obiettivi che persegue; b) il ruolo dei singoli partecipanti e le misure che devono mettere in atto durante la fase preparatoria e in seguito all'attivazione del protocollo di crisi; c) una procedura chiara per stabilire quando debba essere attivato il protocollo di crisi; d) una procedura chiara per determinare il periodo durante il quale devono essere messe in atto le misure da adottare dopo l'attivazione del protocollo di crisi, periodo strettamente limitato a quanto necessario per far fronte alle specifiche circostanze eccezionali in questione; e) le garanzie necessarie per far fronte ad eventuali effetti negativi sull'esercizio dei diritti fondamentali sanciti dalla Carta, in particolare la libertà di espressione e di informazione e il diritto alla non discriminazione; f) una procedura per riferire pubblicamente in merito a tutte le misure adottate, alla loro durata e ai loro esiti, al termine della situazione di crisi. 5. Se ritiene che un protocollo di crisi non affronti efficacemente la situazione di crisi o non garantisca l'esercizio dei diritti fondamentali di cui al paragrafo 4, lettera e), la Commissione chiede ai partecipanti di rivedere tale protocollo, anche adottando misure supplementari». In argomento si veda anche la disamina effettuata nel capitolo 1 del presente report.

[74] In dettaglio, la lett. c) del par. 1 dell'art. 36 del DSA si riferisce alla predisposizione di «una relazione alla Commissione, entro una certa data o a intervalli regolari specificati nella decisione, in merito alle

Ai sensi del par. 3, occorre che le azioni richieste dalla Commissione siano «strettamente necessarie, giustificate e proporzionate» tenuto conto della gravità della minaccia in corso e delle implicazioni, specie per i diritti fondamentali di tutte le parti interessate, delle misure richieste; la Commissione dovrà inoltre indicare «un termine ragionevole entro il quale devono essere adottate le misure specifiche» in questione, anche considerandone l'urgenza e il tempo necessario per la loro preparazione e attuazione; è stabilito in ogni caso che le azioni richieste debbano essere «limitate a un periodo non superiore a tre mesi», eventualmente prorogabili dalla Commissione per un periodo non superiore a ulteriori tre mesi[75]. L'organo di *enforcement* europeo, poi, dovrà monitorare l'applicazione da parte dell'operatore delle misure in parola, avviando se del caso un "dialogo" con quest'ultimo per valutare l'efficacia di tali azioni e richiedendo eventualmente al soggetto regolato di riesaminarle, previa consultazione del Comitato, ferma restando la possibilità, in ogni caso, di revocare la decisione di applicare il meccanismo di risposta alla crisi tenendo conto dell'evoluzione (e specie della cessazione) della situazione emergenziale.

Emerge con chiarezza, tra le righe della disposizione, lo sforzo del legislatore eurounitario di bilanciare le esigenze contrapposte in gioco.

È evidente, invero, come vi sia la consapevolezza dell'attribuzione alla Commissione europea di poteri particolarmente significativi, che gli danno la possibilità di incidere significativamente, con un provvedimento "individuale" e di carattere certamente non poco invasivo, sull'esercizio delle attività di piattaforme online e motori di ricerca di dimensione molto grandi, imponendogli, in tempi molto stretti e con particolare urgenza, l'adozione di diverse misure che presuppongono ponderazioni difficili e scelte molto delicate e complesse alla luce del loro impatto sui diritti fondamentali, specie in simili situazioni d'emergenza. Non è del resto un caso che – tenuto conto delle possibili ripercussioni di tali procedure sia sui diritti delle *corporation* cui vengono richieste le azioni di risposta alla crisi, sia su quelli dei loro utenti che, "di rimbalzo", si troveranno a subire gli effetti dei provvedimenti emergenziali implementati dalle piattaforme e che possono risolversi in significative ingerenze sulla loro sfera giuridica – parte della dottrina abbia subito criticato la genericità e l'ampiezza dei presupposti in grado di inne-

valutazioni di cui alla lettera a), sul contenuto preciso, l'attuazione e l'impatto qualitativo e quantitativo delle misure specifiche adottate a norma della lettera b) e su qualsiasi altra questione connessa a tali valutazioni o misure, come specificato nella decisione».

[75] Il par. 4 dell'art. 36 prevede altresì che «4. A seguito dell'adozione della decisione di cui al paragrafo 1, la Commissione adotta, senza indebito ritardo, tutte le seguenti misure: a) notifica la decisione al fornitore o ai fornitori destinatari della decisione; b) rende la decisione disponibile al pubblico; e c) informa il comitato della decisione, lo invita a presentare il proprio parere e lo tiene informato di eventuali sviluppi successivi relativi alla decisione». In base ai parr. 7, 10 e 11 della medesima previsione, poi, «7. La Commissione monitora l'applicazione delle misure specifiche adottate a norma della decisione di cui al paragrafo 1 del presente articolo sulla base delle relazioni di cui alla lettera c) di tale paragrafo e di ogni altra informazione pertinente, comprese le informazioni che può richiedere a norma dell'articolo 40 o 67, tenendo conto dell'evoluzione della crisi. La Commissione riferisce periodicamente al Comitato in merito a tale monitoraggio, almeno una volta al mese. […] 10. La Commissione tiene nella massima considerazione le raccomandazioni del comitato a norma del presente articolo. 11. La Commissione riferisce al Parlamento europeo e al Consiglio una volta all'anno a seguito dell'adozione di decisioni di cui al presente articolo e, in ogni caso, tre mesi dopo la fine della crisi, in merito all'applicazione delle misure specifiche adottate a norma di tali decisioni».

scare il potere della Commissione di applicare la disposizione in questione[76]. Si pensi, ad esempio, rispetto ai temi della presente ricerca e per meglio chiarire i termini problematici della questione, alla possibilità di applicare tale istituto per "reagire" a campagne di disinformazione su larga scala in occasione di conflitti armati internazionali o pandemie e altre crisi sanitarie gravi, con la richiesta alle piattaforme di modificare le loro condizioni generali d'uso del servizio, con l'effetto di impedire agli utenti di condividere determinate notizie circa lo scontro armato o la minaccia per la salute pubblica in corso; il rischio di forme di indebita censura e di compressione di fondamentali libertà democratiche è in queste ipotesi, evidentemente, tutt'altro che secondario.

Di qui, come forme di *counterbalance*, sia la decisione di perimetrare in un arco temporale molto circoscritto la possibilità di dar corso a tali meccanismi, sia l'importante indicazione di cui al par. 5 dell'art. 36, a tenore del quale la «scelta delle misure specifiche da adottare a norma del paragrafo 1, lettera b), e del paragrafo 7, secondo comma, spetta al fornitore o ai fornitori destinatari della decisione della Commissione»[77]. In linea con un approccio, come visto, che costituisce la cifra dell'intero regolamento, ci pare che tale locuzione debba essere interpretata nel senso che la Commissione possa imporre, nella propria decisione, soltanto l'adozione di un certo e ampio *genus* di misure (ad es., l'adeguamento dei sistemi di raccomandazione delle notizie, oppure delle condizioni generali o delle procedure di moderazione dei contenuti), dovendo essere lasciate al libero apprezzamento del soggetto regolato, in ultima istanza, la costruzione e l'attuazione specifica della *policy*, della misura di dettaglio da adottare, la scelta su "come mettere a terra" concretamente le modifiche delle proprie regole autonormate, senza che i poteri di ingerenza dell'organo pubblico europeo possano spingersi fino a obbligare gli attori privati ad adottare misure "predeterminate", escludendo qualsiasi margine di scelta su come implementare e integrare il tipo di provvedimenti richiesti all'interno del proprio contesto operativo interno.

[76] V. in particolare V. Colarocco - M. Cogode, *Gli obblighi applicabili a piattaforme* online *di dimensioni molto grandi (Artt. 33-43 – Capo III, Sezione 5)*, in *Diritto di internet*, 1, 2023, 32, ove si è osservato che «Le decisioni che riguardano la libertà di espressione e l'accesso alle informazioni, in particolare in tempi di crisi, non possono essere legittimamente prese dal solo potere esecutivo ma occorre un controllo parlamentare sull'esistenza e sulla durata della situazione emergenziale al fine di evitare abusi. La definizione di crisi deve, infatti, soddisfare i principi di chiarezza e specificità e non deve autorizzare la Commissione a mantenere misure di crisi per un periodo prolungato o indefinito. La definizione dovrebbe quindi, nella concreta interpretazione che ne verrà fornita, essere limitata alle minacce che sono in grado di destabilizzare seriamente le strutture costituzionali, politiche, economiche o sociali fondamentali dell'Unione o parti significative di esse. E il meccanismo proposto dovrebbe, a sua volta e per logica conseguenza, prevedere un ruolo più centrale degli organi rappresentativi dei cittadini, sottraendo all'esecutivo il potere unilaterale di limitare in modo quasi permanente l'accesso del pubblico alle informazioni e alla loro diffusione».

[77] Il par. 1 della stessa disposizione prevede altresì che «Nell'individuare e applicare le misure di cui alla lettera b) del presente paragrafo, il prestatore o i prestatori di servizi tengono debitamente conto della criticità della grave minaccia di cui al paragrafo 2, dell'urgenza delle misure e delle implicazioni effettive o potenziali per i diritti e gli interessi legittimi di tutte le parti interessate, compresa l'eventuale inosservanza dei diritti fondamentali sanciti dalla Carta».

4.4. L'*independent audit*

L'art. 37 del DSA, facendo propria una tipica metodologia della *corporate compliance*, sancisce l'obbligo per le piattaforme online e i motori di ricerca di dimensioni molto grandi di sottoporsi, a proprie spese «e almeno una volta all'anno», a *independent audit*[78] – effettuati da organizzazioni che soddisfino requisiti di indipendenza, comprovata esperienza, obiettività e deontologia professionale dettagliatamente normati dal par. 3 della disposizione[79] – volti a valutare la conformità dell'organizzazione: «a) agli obblighi stabiliti al capo III; b) agli impegni assunti a norma dei codici di condotta di cui agli articoli 45 e 46 e dei protocolli di crisi di cui all'articolo 48».

Al termine dell'attività di revisione, tali organismi redigeranno una relazione finale, che conterrà un giudizio circa il rispetto, da parte del soggetto regolato, dei detti obblighi stabiliti dal regolamento.

L'esito finale di tale revisione, in particolare, potrà essere «positivo», «positivo con osservazioni», o «negativo», in questi ultimi due casi dovendosi naturalmente fornire «raccomandazioni operative su misure specifiche per conseguire la conformità e sui tempi raccomandati per conseguirla»[80], con l'obbligo per le organizzazioni in questione

[78] La previsione fornisce naturalmente ulteriori dettagli sia rispetto agli obblighi di cooperazione delle piattaforme nello svolgimento delle revisioni, sia con riferimento alla trasparenza e agli aspetti di riservatezza e segreto professionale correlati a tali attività, stabilendo in particolare al par. 2 che «I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi consentono alle organizzazioni che effettuano le revisioni a norma del presente articolo la cooperazione e l'assistenza necessarie per consentire loro di svolgere tali revisioni in modo efficace, efficiente e tempestivo, anche provvedendo a dare loro accesso a tutti i dati e ai locali pertinenti, e rispondendo a domande orali o scritte. Essi si astengono dall'ostacolare, influenzare indebitamente o compromettere lo svolgimento della revisione. Dette revisioni garantiscono un adeguato livello di riservatezza e il segreto professionale per quanto riguarda le informazioni ottenute dai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi e da terzi nel contesto delle revisioni, anche dopo la loro conclusione. Tuttavia, il rispetto di tale obbligo non deve pregiudicare l'esecuzione delle revisioni e delle altre disposizioni del presente regolamento, in particolare quelle in materia di trasparenza, vigilanza ed esecuzione. Se necessario ai fini della relazione sulla trasparenza a norma dell'articolo 42, paragrafo 4, la relazione di revisione e la relazione di esecuzione della revisione di cui ai paragrafi 4 e 6 del presente articolo sono accompagnate dalle versioni prive di informazioni che potrebbero essere ragionevolmente considerate riservate».

[79] Ove è stabilito che «Le revisioni effettuate a norma del paragrafo 1 sono eseguite da organizzazioni: a) indipendenti e in assenza di conflitti di interessi con il fornitore di piattaforme online di dimensioni molto grandi o di motori di ricerca online di dimensioni molto grandi in questione, e con qualsiasi persona giuridica connessa con tale fornitore; in particolare: i) non devono aver fornito servizi diversi dalla revisione relativi alle questioni sottoposte a revisione al fornitore della piattaforma online di dimensioni molto grandi interessata o del motore di ricerca online di dimensioni molto grandi in questione e a qualsiasi persona giuridica collegata a tale fornitore nei 12 mesi precedenti l'inizio della revisione, e devono essersi impegnati a non fornire tali servizi nei 12 mesi successivi al completamento della revisione; ii) non devono aver fornito servizi di revisione a norma del presente articolo al fornitore della piattaforma online di dimensioni molto grandi interessata o del motore di ricerca online di dimensioni molto grandi in questione e a qualsiasi persona giuridica collegata a tale fornitore per un periodo superiore a dieci anni consecutivi; iii) non possono effettuare la revisione a fronte di corrispettivi che dipendono dall'esito dello stesso; b) sono dotate di comprovata esperienza nel settore della gestione dei rischi, di competenze e di capacità tecniche; c) sono dotate di comprovata obiettività e deontologia professionale, basata in particolare sull'adesione a codici di condotta o standard appropriati».

[80] In dettaglio i parr. 4 e 5 dell'art. 37 del DSA prevedono che «4. I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi provvedono affinché le organizzazioni che effettuano le revisioni redigano una relazione per ciascuna revisione. Tale relazione

di tener «debitamente conto» di queste ultime e di adottare, entro «un mese dal ricevimento di tali raccomandazioni» una «relazione di attuazione della revisione con cui stabiliscono tali misure» oppure forniscono adeguata giustificazione delle ragioni per cui ritengono di non darvi corso, descrivendo, tuttavia, le «misure alternative» adottate per risolvere tutte le "*instances of non-compliance*" che siano state identificate[81]. Quest'ultima specificazione, in particolare, costituisce l'ennesima conferma della scelta del legislatore eurounitario di non imporre mai l'adozione di specifiche *policy* di dettaglio, lasciando sempre alle piattaforme la decisione definitiva sulle modalità concrete di adempimento ai doveri di *due diligence* loro imposti.

Si tratta, in definitiva, di una disposizione "di chiusura" che, unitamente all'art. 41 del DSA relativo all'istituzione di una specifica *compliance function* aziendale, sul quale subito ci soffermeremo[82], completa il novero degli obblighi gravanti sui grandi *player* del mercato digitale, chiamati a confrontarsi con organismi indipendenti esterni in merito alla correttezza del proprio apparato rispetto a quanto richiesto dal nuovo regolamento europeo. È un ulteriore *step* di una strategia di regolazione volta a garantire il più possibile l'effettività e la correttezza del *private enforcement* di operatori il cui impegno proattivo sarà essenziale per consentire il raggiungimento degli obiettivi della riforma[83].

è motivata per iscritto e contiene almeno gli elementi seguenti: a) il nome, l'indirizzo e il punto di contatto del fornitore della piattaforma online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi oggetto della revisione e il periodo di riferimento della revisione; b) il nome e l'indirizzo dell'organizzazione o delle organizzazioni che eseguono la revisione; c) una dichiarazione di interessi; d) una descrizione degli elementi specifici sottoposti a revisione e della metodologia applicata; e) una descrizione e una sintesi delle principali constatazioni derivanti dalla revisione; f) un elenco delle parti terze consultate nel quadro della revisione; g) un giudizio di revisione sul rispetto, da parte del fornitore della piattaforma online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi oggetto della revisione, degli obblighi e degli impegni di cui al paragrafo 1, giudizio che può essere segnatamente «positivo», «positivo con osservazioni» o «negativo»; h) se il giudizio di revisione non è «positivo», raccomandazioni operative su misure specifiche per conseguire la conformità e sui tempi raccomandati per conseguirla. 5. Qualora l'organizzazione che ha effettuato la revisione non abbia potuto verificare determinati elementi specifici o esprimere un giudizio di revisione sulla base delle proprie indagini, la relazione di revisione include una spiegazione delle circostanze e dei motivi per cui tali elementi non hanno potuto essere sottoposti a revisione».

[81] Ai sensi del par. 7 dell'art. 37 del DSA, peraltro, e in linea con altre analoghe previsioni del regolamento, viene conferito alla Commissione europea «il potere di adottare atti delegati conformemente all'articolo 87 al fine di integrare il presente regolamento stabilendo le norme necessarie per lo svolgimento delle revisioni a norma del presente articolo, in particolare per quanto riguarda la regolamentazione necessaria per le fasi procedurali, le metodologie di revisione e i modelli di comunicazione delle revisioni effettuate a norma del presente articolo. Tali atti delegati tengono conto di eventuali standard di revisione volontari a norma dell'articolo 44, paragrafo 1, lettera e)».

[82] Cfr. il paragrafo successivo.

[83] In dottrina, ad ogni modo, non si è mancato di identificare alcuni possibili rischi, nella misura in cui «*VLOPs may leverage their market power against their new mandatory auditors and risk assessors, a threat theorised as 'audit capture'*»: cfr. J. Laux - S. Wachter - B. Mittelstadt, *Taming the few: Platform regulation, independent audits, and the risks of capture created by the DMA and DSA*, in *Computer Law & Security Review*, 1, 2021, 43.

4.5. L'istituzione di una specifica funzione aziendale di *compliance* per monitorare la conformità dell'organizzazione agli obblighi del DSA

L'art. 41 del DSA, come anticipato, "chiude" il cerchio degli obblighi aggiuntivi gravanti sulle piattaforme online e sui motori di ricerca di dimensioni molto grandi, stabilendo che questi ultimi debbano istituire una specifica *compliance function* al fine di monitorare la conformità dell'organizzazione agli obblighi sanciti dal nuovo regolamento; dovrà trattarsi di una articolazione societaria indipendente dalle funzioni operative, composta da uno o più "*compliance officer*s", compreso l'*head* di tale "ufficio" (quale figura che in qualche modo si 'ispira' a quella del DPO in ambito *privacy*).
La previsione in questione, in linea con le consolidate *best practice* in tema di *corporate governance*, delinea una funzione di controllo a diretto riporto dell'organo di gestione, composta, quanto all'*head*, da un «un alto dirigente indipendente con responsabilità distinta per la funzione di controllo della conformità», nonché, quanto ad ogni altro componente, da soggetti in possesso delle «qualifiche professionali, delle conoscenze, dell'esperienza e delle capacità necessarie».
L'organo di gestione manterrà la responsabilità ultima in ordine alla approvazione e al riesame periodico delle strategie di valutazione, gestione e monitoraggio dei rischi (in particolare quelli di cui all'art. 34 del DSA), nonché rispetto alla costruzione di sistemi di *governance* che garantiscano, anche tramite la separazione delle responsabilità e la prevenzione dei conflitti di interesse, l'indipendenza della funzione di DSA *compliance* e l'assegnazione ai relativi *officer* di risorse, *status* e poteri necessari per adempiere alle proprie funzioni[84].
I compiti di tale funzione di *compliance* consistono, appunto, nel vigilare sul rispetto da parte della *corporation* delle *obligation* sancite dal DSA. In particolare, tale organismo sarà chiamato a: collaborare con il coordinatore dei servizi digitali del luogo di stabilimento e con la Commissione; assicurare il corretto svolgimento delle attività di *risk assessment* e *management* di cui agli artt. 34 e 35 del DSA; organizzare e sovraintendere agli adempimenti connessi agli *independent audit* di cui all'art. 37; informare e consigliare i dirigenti e i dipendenti dell'organizzazione in merito agli obblighi del regolamento ed esercitare un ruolo di impulso nei confronti dell'organo di gestione rispetto a tutte le questioni connesse alla DSA *compliance*; monitorare la conformità agli obblighi connessi ai codici di condotta e ai protocolli di crisi *ex* artt. 45 e ss. del DSA.
A fronte dell'inesistenza di un *dovere generale* per le società di istituire una simile funzione societaria, come noto resa obbligatoria esclusivamente in specifici ambiti settoriali[85], è quindi molto significativo notare come il legislatore europeo abbia scelto qui di rendere cogente la sua costituzione, con una decisione che è del resto in linea, come detto, con le *policy* fatte proprie da fonti normative analoghe; la presenza di un punto

[84] Si prevede, inoltre, che l'*head* della funzione di *compliance* non possa essere rimosso senza previa approvazione dell'organo di gestione e l'obbligo per i soggetti di regolati di comunicare nominativo e riferimenti di tale soggetto al coordinatore dei servizi digitali del luogo di stabilimento e alla Commissione europea.

[85] Cfr. chiaramente, ad esempio, l'art. 7 del Codice di autodisciplina delle società quotate italiane, reperibile in *borsaitaliana.it*.

di riferimento unico all'interno dell'organizzazione, che sovraintenda alle varie attività di controllo della conformità, e svolga un ruolo di impulso e di coordinamento complessivo dei correlati adempimenti, facendo da "collettore" delle varie istanze, è invero giustamente considerata un passaggio essenziale di completamento della disciplina, a presidio della sua efficacia.

Sarà, per il resto, importante verificare come la prassi si orienterà rispetto all'organizzazione e al funzionamento concreto della funzione di DSA *compliance*.

Due ci sembrano gli aspetti più rilevanti.

Anzitutto, la lettera del regolamento consente espressamente di scegliere tra una composizione monocratica o collegiale. Se da un lato una maggiore flessibilità può sembrare apprezzabile, di contro è molto difficile ipotizzare che, nel contesto di *corporation* di "dimensioni molto grandi", un unico funzionario possa assicurare uno svolgimento realmente efficace dei compiti assegnati a tale articolazione in organizzazioni complesse con una considerevole mole di utenti e, quindi, di *workflow*. Ci sembra sia preferibile allora, quantomeno di regola, optare per la nomina di plurimi responsabili, in numero adeguato alle specificità di ogni operatore.

In secondo luogo, in base la lettera del regolamento non è chiaro se debba trattarsi di un organismo da istituire totalmente *ex novo*, o se le responsabilità definite dall'art. 41 DSA possano essere assegnate a o uno o più componenti delle funzioni di *compliance* eventualmente già esistenti nelle organizzazioni (come è molto probabile che sia in enti di questo tipo), sempre, naturalmente, a condizione che tali uffici e i loro singoli membri – che la piattaforma voglia designare come DSA *compliance officer* – soddisfino i predetti requisiti delineati dal nuovo regolamento europeo. Il testo originale, che utilizza la locuzione «*shall establish*» ("istituiscono" nella traduzione italiana), non pare offrire certezze in merito, pur sembrando maggiormente "evocare"[86], almeno a livello strettamente letterale, la creazione di una nuova struttura. Tuttavia, a noi pare sia ragionevole (e conforme alla *ratio* del regolamento[87]) considerare legittima la seconda soluzione, se del caso costruendo un *team* "*ad hoc*" all'interno dell'ufficio già presente, anche per assicurare una ragionevole allocazione delle risorse organizzative e finanziarie e lo sfruttamento di quelle già esistenti, nell'ottica di una *compliance* realmente integrata quale approccio ormai indispensabile in uno scenario regolatorio sempre più complesso e variegato per i soggetti metaindividuali.

5. Riflessioni conclusive e indicazioni di *policy*

Il DSA è riuscito a colmare una significativa lacuna che caratterizzava lo scenario normativo europeo e di diversi Stati membri, in un panorama regolamentare in cui si erano iniziate ad affacciare, a "macchia di leopardo" e in singoli ordinamenti, iniziati-

[86] A conclusioni diverse si sarebbe senza alcun dubbio giunti nel caso di utilizzo di termini più neutri come "designare" o "nominare" ("*appoint*" in lingua inglese).

[87] Del resto, ciò in qualche modo potrebbe contribuire anche a chiarire la ragione per cui il DSA consente di nominare anche un solo responsabile della conformità.

ve legislative parziali[88], che toccavano solo alcuni punti dei profili poi organicamente ricondotti ad unità dalla nuova normativa eurounitaria; ciò anche con riferimento alla responsabilizzazione degli operatori digitali nelle attività di autonormazione e auto-organizzazione che abbiamo descritto in questa parte della ricerca. Ed è peraltro molto importante che ci si sia fatti carico di risolvere tale *gap* mediante un regolamento europeo, trattandosi di uno strumento per definizione più adatto a disciplinare un fenomeno, afferente ai più importanti modelli di *business* digitali, per sua natura transnazionale e che necessita, inevitabilmente, di risposte di pari respiro e non già esclusivamente "locali".

Anche solo guardando alla situazione immediatamente precedente l'approvazione del DSA, quindi, si può essere soddisfatti dei risultati raggiunti. La sensazione è quella di essere di fronte a un prodotto normativo di buona fattura, pure al netto di alcune criticità che abbiamo cercato di porre in evidenza e che forse, in fin dei conti, sono del tutto comprensibili in un atto legislativo che è stato giustamente ed efficacemente definito come "pioneristico"[89]. Insomma, si tratta di un percorso in cui, nel complesso, le luci prevalgono sulle ombre.

Giunti alla fine di questo contributo, non resta allora che tentare di fornire alcune indicazioni di *policy* che confluiranno nel documento contenuto in calce allo studio in cui, come per gli scorsi cicli della ricerca, avremo cura di tesaurizzare i risultati delle indagini condotte nelle varie sezioni in cui è stata articolata la nostra disamina del DSA, costruendo un prospetto unitario di raccomandazioni rivolte ai vari attori del settore.

Procediamo con ordine, ripercorrendo nella stessa "direzione di marcia" fin qui seguita i vari temi di cui ci siamo occupati in questo lavoro e cercando di isolare le questioni maggiormente importanti dall'angolo visuale del contrasto alla disinformazione.

Quattro sono gli aspetti su cui, a nostro avviso, occorre concentrare l'attenzione.

Un primo tema attiene alla definizione di termini e condizioni del servizio (c.d. standard della *community*). Qui, come visto[90], le piattaforme dovrebbero rafforzare l'apparato di garanzie minime definito dall'art. 14, disciplinando l'esercizio dei propri poteri "sanzionatori" nel rispetto di diritti essenziali che devono necessariamente essere riconosciuti nell'implementazione di qualsiasi paradigma punitivo, anche in ambito privato: la legalità delle violazioni e delle misure sanzionatorie/interdittive, con i corollari della irretroattività, della tassatività/precisione delle previsioni punitive e del divieto di analogia; la dettagliata definizione dei soggetti titolari della potestà di dettare tali regole; il principio di proporzionalità del trattamento sanzionatorio; il divieto di responsabilità oggettiva e l'affermazione del principio di colpevolezza, etc.

Per ciò che concerne nello specifico la strutturazione di *policy* anti-disinformazione può essere rischioso e controproducente limitarsi a prevedere un generale divieto per

[88] Cfr. *supra* par. 1. Per un'analisi che ha messo in evidenza tale evoluzione del panorama normativo europeo, anche con richiami ad alcuni «*worrying trends toward criminalisation*», v. R. Ò Fathaigh - N. Helberger - N. Appelman, *The perils of legally defining disinformation*, in *Internet Policy Review*, 10(4), 2021, 2 ss.

[89] V. l'introduzione alla presente ricerca di A. Gullo, *Contenuti, scopi e traiettoria della ricerca*, cit. Non a caso in dottrina si è rilevato come «*the DSA is likely to shape the global approach to content regulation in this emerging area of law*»: cfr. P. Church - C.N. Pehlivan, *The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability*, in *Global Privacy Law Review*, 4(1), 2023, 53 ss.

[90] Cfr. *supra* par. 1.1.

gli utenti, invero troppo ampio e indeterminato, di condivisione di notizie false. La difficoltà, come sappiamo[91], di segnare un preciso confine tra esternazioni di fatti e opinioni personali, oggettivo e soggettivo, vero e falso, finirebbe per rendere tale "regola interna" difficilmente attuabile dai soggetti chiamati, all'interno dell'organizzazione, a moderare i contenuti immessi in rete dagli utenti e, soprattutto, per risolversi in molti casi in una indebita compressione della libertà di espressione dei destinatari del servizio.

Nella strutturazione di *term and conditions*, da tale specifica prospettiva, occorre allora introdurre divieti ben circostanziati, circoscritti, tassativi, con un approccio *case by case* e procedendo per singoli settori sensibili, vietando, ad esempio, l'intenzionale condivisione di notizie obiettivamente qualificabili come non vere per cui si riportino inesistenti difficoltà di accesso ai seggi elettorali o nelle operazioni di voto, con l'obiettivo di disincentivare le persone a recarsi alle urne e ledendo quindi l'interesse all'integrità ai processi elettorali, o notizie di analogo tenore volte ad arrecare pregiudizio a campagne vaccinali a tutela della salute pubblica, e così via.

Ancora, non dovrebbero essere consentite, a prescindere dal contenuto della notizia condivisa (e dalla sua veridicità), specifiche modalità decettive di utilizzo del servizio come l'interazione artificiosa tra più *account* o l'uso di *bot* automatici al fine di aumentare fraudolentemente la visibilità di certe informazioni.

I settori sensibili nei quali disciplinare e applicare tali politiche interne di gestione del servizio, inoltre, andrebbero identificati tramite un'analisi dei rischi svolta secondo i criteri di cui all'art. 34 DSA, le cui indicazioni di metodo dovrebbero essere seguite anche da piattaforme e motori di ricerca non qualificati come organizzazioni di "dimensioni molto grandi", pur, naturalmente, tenendo conto delle proprie specificità operative e organizzative e adattando di conseguenza i detti principi di *assessment*. Bisognerà poi coordinare la costruzione di tali standard della *community* con le conseguenti misure di mitigazione del rischio anche sul versante tecnico[92], tra cui la riduzione della visibilità o la c.d. demonetizzazione dei contenuti, la revisione dei sistemi di raccomandazione e pubblicità per evitare che dette informazioni diventino virali, l'utilizzo di contrassegni ben visibili per consentire agli utenti di identificare chiaramente i c.d. *deep fake* (e per dare la possibilità agli autori di *post* che li immettano in rete di indicare chiaramente la loro natura "falsa"[93]), unitamente a ogni altro accorgimento, sul piano del funzionamento concreto del servizio, indispensabile per rendere tale *enforcement* realmente efficace.

Una seconda questione concerne i meccanismi di *notice and action*: abbiamo infatti rile-

[91] Per una più ampia disamina, e altri riferimenti bibliografici, sia consentito rinviare ancora a E. Birritteri, *Punire la disinformazione*, cit., 304 ss.

[92] Per un inquadramento di queste misure, con particolare riferimento ai filtri tecnici, v. M. Steinebach, *Potential and Limits of Filter Technology for the Regulation of Hate Speech and Fake News*, in A. von Ungern-Sternberg (a cura di), *Content Regulation in the European Union*, cit., 13 ss.

[93] L'art. 35, par. 1, lett. k), del DSA si riferisce, come abbiamo già evidenziato, al ricorso «a un contrassegno ben visibile per fare in modo che un elemento di un'informazione, sia esso un'immagine, un contenuto audio o video, generati o manipolati, che assomigli notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che a una persona appaia falsamente autentico o veritiero, sia distinguibile quando è presentato sulle loro interfacce online e, inoltre, la fornitura di una funzionalità di facile utilizzo che consenta ai destinatari del servizio di indicare tale informazione».

vato[94] che rispetto al contrasto alla disinformazione diversi contenuti o modalità d'utilizzo del servizio non possono spesso dirsi di per sé illegali; di conseguenza, le piattaforme online dovrebbero rendere disponibili i propri sistemi interni di segnalazione anche per l'invio di report che evidenzino semplicemente l'incompatibilità del contenuto con i c.d. standard della *community* (e in particolare con le *policy* dettate in materia di condivisione di notizie false).

Un terzo punto cruciale riguarda i sistemi interni di gestione dei reclami, trattandosi di un profilo particolarmente delicato dell'*enforcement* privato delle politiche anti-disinformazione, alla luce della tensione che inevitabilmente si genera tra esse e il rispetto della libertà di espressione. Per tali ragioni, anche in tal caso a nostro avviso è necessario che le piattaforme assicurino un livello maggiore di garanzie rispetto a quello minimo richiesto dagli artt. 17 e 20 del DSA, assicurando agli utenti, tra l'altro, un pieno contraddittorio preventivo, la garanzia di sufficiente autonomia e indipendenza (con riferimento alla distribuzione dei poteri dell'organizzazione) dei soggetti deputati a irrogare la sanzione e a decidere sui connessi reclami, il diritto di richiedere il riesame della decisione già a livello interno[95].

Un ultimo aspetto, infine, è quello legato al rafforzamento degli strumenti di monitoraggio continuo dell'efficacia dell'apparato di DSA *compliance* realizzato da queste organizzazioni[96], essendo auspicabile che anche piattaforme e motori di ricerca non designati come operatori "di dimensioni molto grandi" nominino *compliance officer* dedicati e si sottopongano, ove possibile, ad *audit* interni ed esterni indipendenti su base volontaria, pur con un approccio improntato a un'ampia flessibilità e alla possibilità di modellare gli adempimenti alla luce delle proprie specificità. Considerata la natura estremamente sensibile di tali pratiche di autonormazione, e per certi versi anche l'indubbia difficoltà di implementare una strategia di contrasto alla disinformazione, infatti, appare essenziale non soltanto avvalersi di figure incaricate di monitorare la conformità dell'organizzazione agli obblighi del DSA, e la loro efficace attuazione, ma anche favorire un proficuo confronto tra la *corporation* e i vari attori del sistema, dal momento che solo una ampia e costante cooperazione tra i diversi *stakeholder* potrà realmente assicurare il raggiungimento degli obiettivi che questa ambiziosa riforma ha cercato di conseguire all'esito di un difficile bilanciamento di tutti gli interessi in gioco.

[94] Cfr. *supra* par. 2.1.

[95] V. anche *supra* par. 3.1.

[96] Cfr. *supra* parr. 4.4 e 4.5.

L'*enforcement* pubblico del *Digital Services Act* tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni*

Rossella Sabia

Abstract

Il contributo offre una panoramica sui caratteri di fondo del regolamento (UE) 2022/2065 (*Digital Services Act* – DSA) con riguardo all'architettura dei poteri di *enforcement* sul versante pubblico e del riparto di competenze tra livello nazionale ed europeo (Capo IV, dedicato all'attuazione, alla cooperazione, alle sanzioni e all'esecuzione del DSA). Si tratta di un ambito di sicuro interesse per il penalista, intercettando la questione dello spazio riservato – nella tutela sia dei diritti degli utenti di servizi digitali, sia delle funzioni delle autorità coinvolte – alla risposta sanzionatoria che – pur non ricorrendosi qui al diritto criminale – presenta non trascurabili connotati di afflittività. Il lavoro muove dal contesto nazionale, con riferimento alla figura del coordinatore dei servizi digitali; esamina il ruolo da protagonista della Commissione europea nei rapporti con le piattaforme di dimensioni molto grandi; discute il 'livello intermedio' costituito dal Comitato europeo per i servizi digitali, restituendo chiara la dimensione collaborativa e la struttura 'a rete' della *governance* tratteggiata dal Regolamento.

This article aims at outlining the main features of the Regulation (EU) 2022/2065 (*Digital Services Act* – DSA) with regard to the architecture of the public enforcement and the distribution of competences between national and EU levels (Chapter IV, dedicated to the implementation, cooperation, penalties and enforcement of the DSA).

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco". Il presente report costituisce la sezione giuridica del terzo ciclo della ricerca dal titolo "Come individuare e contrastare operazioni coordinate di disinformazione in Italia. Casi di studio e indicazioni di policy per istituzioni pubbliche e private", condotta nell'A.A. 2022/2023 da ricercatori dell'Università Luiss Guido Carli, della Harvard Kennedy School e della School of Information dell'Università del Michigan. La ricerca è stata realizzata con un contributo dell'Unità di Analisi, Programmazione e Documentazione Storica del Ministero italiano degli Affari Esteri e della Cooperazione Internazionale (MAECI), ai sensi dell'art. 23-bis del d.p.r. n. 18 del 5 gennaio 1967. Le riflessioni contenute in questa ricerca riflettono esclusivamente la visione degli autori e non sono necessariamente rappresentative dell'opinione del MAECI e delle altre istituzioni coinvolte. Si ringraziano l'Unità di Analisi, Programmazione e Documentazione Storica del MAECI e gli altri Direttori della ricerca (Irene Pasquetto, Gianni Riotta e Costanza Sciubba Caniglia) per avere consentito la pubblicazione degli scritti in questa sede.

This is an interesting area for criminal law scholars, as it involves the question of the role of penalties in the DSA – for the protection of both the rights of users of digital services and the functions of the authorities involved –; although not criminal in nature, they show a certain degree of severity. The contribution starts from the national context, with reference to digital services coordinators; it examines the leading role of the European Commission in relation with very large online platforms; it discusses the "intermediate level" represented by the European board for Digital Services, thus highlighting the collaborative dimension and the "network" structure of the governance outlined by the Regulation.

Sommario

Keywords

Digital Services Act – *Public enforcement* – Coordinatori dei servizi digitali – Commissione europea – Sanzioni

1. L'*enforcement* pubblico del *Digital Services Act*: un inquadramento generale

Il *Digital Services Act* (DSA)[1], pubblicato nella Gazzetta ufficiale dell'Unione europea a ottobre 2022, rappresenta il più grande cambiamento di regole, da vent'anni a questa parte, per la responsabilità degli intermediari online, recando un nuovo e composito quadro normativo che – attraverso l'introduzione di rilevanti obblighi e doveri di diligenza a carico dei *provider* – ha l'obiettivo di contemperare esigenze diverse: appron-

[1] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (Regolamento sui servizi digitali). Per una recente panoramica sulla nuova normativa v. il volume collettaneo a cura di A. Von Ungern-Sternberg, *Content Moderation in the EU: The Digital Services Act*, *Trier Studies on Digital Law*, Trier, 2023, nonché quello a cura di J. Van Hoboken e altri, *Putting the Digital Services Act into Practice: Enforcement, Access to Justice, and Global Implications*, Berlin, 2023. Nel contesto italiano, v. i diversi contributi pubblicati nel fascicolo n. 1/2023 di *Diritto di internet*, oltre alla circolare Assonime n. 17/2023 "Mercato Unico dei servizi digitali: il Digital Services Act" del 12 giugno 2023.

tare una risposta ai rischi causati da contenuti generati dagli utenti, proteggere i diritti fondamentali, con particolare riguardo alla libertà di espressione, trovare soluzioni ai limiti pratici della moderazione dei contenuti su scala[2].

Tale intervento si inscrive nell'ambito della strategia dell'Unione europea[3] volta a gettare le basi, anticipando altri Paesi del mondo, per l'affermazione di una «compiuta politica pubblica digitale», perseguendo sia il consolidamento della *leadership* globale nel settore della regolazione delle piattaforme, sia il contenimento del proliferare di discipline nazionali in materia – come ad esempio quelle tedesca o francese – che potrebbero condurre a una problematica disomogeneità di approcci nel mercato interno[4].

Come è stato bene messo in evidenza in altre sezioni di questa ricerca, il DSA – pur ponendosi, per diversi profili, in continuità con la pregressa disciplina contenuta nella direttiva 2000/31/CE sul commercio elettronico, come accade ad esempio in relazione alla responsabilità del *provider*[5] – introduce innovazioni degne di nota specialmente sul terreno degli obblighi di *due diligence* posti in capo agli intermediari di servizi digitali, soprattutto per ciò che concerne le restrizioni alle informazioni condivise dagli utenti [6]. Sul punto, occorre ricordare che si tratta di doveri asimmetrici[7], a pervasività crescente e progressiva in rapporto alla natura dei servizi prestati e alle dimensioni del fornitore, arrivando il regolamento, con specifico riferimento alle c.d. «*very large online platforms*» – ossia quelle aventi un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a quarantacinque milioni e designate come tali dalla Commissione europea[8] – a stabilire regole *ad hoc* nel Capo III, sezione 5 del DSA, su cui vigila in via esclusiva, come si vedrà, la Commissione europea[9].

Questa opzione di *policy* muove dalla presa d'atto dell'insufficienza delle sole misure

---

[2] Questa la sintesi efficace di P. Church - C. Pehlivan, *The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability*, in *Global Privacy Law Review*, 4(1), 2022, 53, i quali definiscono appunto il DSA «*the biggest shake up to the rules for online intermediary liability in twenty years*». Per una analisi del regolamento con un focus sul suo impatto etico-sociale, si rinvia a A. Turillazzi - M. Taddeo - L. Floridi - F. Casolari, *The Digital Services Act: An Analysis of its Ethical, Legal, and Social Implications*, in *Law, Innovation and Technology*, 15, 2023, 83 ss.

[3] Per un ampio inquadramento del ruolo dell'Unione europea nello scenario globale sul versante digitale, v. E. Fahey, *The EU as a Global Digital Actor. Institutionalising Global Data Protection, Trade, and Cybersecurity*, Oxford, 2022; A. Manganelli - A. Nicita, *Regulating Digital Markets. The European Approach*, Cham, 2022. Nella prospettiva di un raffronto tra il DSA e l'esperienza statunitense v. D. C. Nunziato, *The Digital Services Act and the Brussels Effect on Platform Content Moderation*, in *Chicago Journal of International Law*, 24(1), 2023, 115 ss.

[4] G. Buttarelli, *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche*, in *Giornale di diritto amministrativo*, 1, 2023, 120, richiama in particolare il *NetzDG* tedesco del 2017 in tema di obblighi di rimozione dei contenuti illeciti online e la *Loi Avia* francese del 2020.

[5] L. D'Agostino, *Disinformazione e obblighi di* compliance *degli operatori del mercato digitale alla luce del nuovo* Digital Services Act*,* in questa medesima sezione monografica, in questa *Rivista*, 2, 2023.

[6] Del tema si occupa E. Birritteri, *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di* compliance *e dei poteri di autonormazione degli operatori,* in questa medesima sezione monografica, in questa *Rivista*, 2, 2023.

[7] F. G'sell, *The Digital Services Act: a General Assessment*, in A. Von Ungern-Sternberg (a cura di), *Content Moderation in the EU*, cit., 88 ss.

[8] V. E. Birritteri, *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di* compliance *e dei poteri di autonormazione degli operatori,* cit., par. 4.

[9] *Infra*, par. 6 e 6.1.

di autoregolazione da parte delle piattaforme per limitare la diffusione di *illegal content* e dalle criticità connesse ai caratteri che detta *self-regulation* è andata assumendo. In proposito, si parla di «sovranità digitale» in capo a tali soggetti, che hanno finito per accentrare su di sé la definizione di regole generali, il controllo sul loro rispetto, la costruzione di apparati in linea di massima indipendenti per la risoluzione di eventuali controversie, così mimando «il potere pubblico […] anche se tutte le funzioni […] sono strutturate e rimangono all'interno della piattaforma», che presenta «i tratti tipici di un ordinamento giuridico, autonomo dall'ordinamento generale»[10].

Il DSA denota dunque una significativa volontà di riaffermazione del ruolo della eteroregolazione nel campo dei servizi digitali, delineando per la prima volta in modo strutturato una cornice di regole di fonte pubblicistica entro cui incasellare le pratiche di *private enforcement* degli operatori – attuate mediante la moderazione dei contenuti immessi online degli utenti, con un rilevante impatto sull'esercizio di diritti fondamentali – come detto, *freedom of speech in primis*[11] – e fissando i criteri di riferimento delle scelte di *self-policing* e dei poteri *lato sensu* "sanzionatori" delle piattaforme[12].

Il risultato è un apparato di regole alla ricerca di un equilibrio nella composizione di tale dualismo pubblico-privato, nel segno, anzitutto, di un ruolo attivo dei destinatari della disciplina – i c.d. servizi di intermediazione[13] – cui il DSA impone una serie di obblighi (si è parlato di «*layer cake*»)[14] stratificati dal basso verso l'alto, *id est* regole variabili in base alle caratteristiche del *provider* e via via più complesse, per cui il soggetto che si trovi al vertice è tenuto osservare sia le disposizioni specifiche per la propria attività, sia quelle dettate per i soggetti collocati ai livelli inferiori[15]. Come anticipato, si arriva ad affidare ai *player* di dimensioni molto grandi doveri *aggiuntivi*, quali la mappatura e gestione dei rischi sistemici, il sottoporsi a *audit* indipendenti e la costituzione di una

[10] L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Rivista trimestrale di diritto pubblico*, 4, 2022,1103 s. Rispetto ai riflessi di tali poteri sul versante sanzionatorio v. già E. Birritteri, *Punire la disinformazione: il ruolo del diritto penale e delle misure di moderazione dei contenuti delle piattaforme tra pubblico e privato*, in *Diritto penale contemporaneo – Rivista Trimestrale*, 4, 2021, 304 ss.

[11] Per alcune notazioni critiche sull'approccio europeo al tema, v. V. Zeno-Zencovich, *The EU Regulation of Speech. A Critical View*, in questa *Rivista*, 1, 2023, 11 ss.

[12] V. sul punto E. Birritteri, *Contrasto alla disinformazione*, Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di* compliance *e dei poteri di autonormazione degli operatori*, cit.

[13] Per la definizione, cfr. art. 3, par. 1, lett. *g)*, DSA, a norma del quale vi rientrano servizi della società dell'informazione quali il semplice trasporto (*mere conduit*), consistente nella trasmissione di informazioni su una rete di comunicazione o nella fornitura di accesso a una rete di comunicazione (*i*), la memorizzazione temporanea (*caching*) (*ii*) e la memorizzazione di informazioni fornite dagli utenti (*hosting*) (*iii*). A queste categorie, già presenti nella direttiva sul commercio elettronico, si aggiungono quelle del medesimo articolo, lett. *i)* e lett. *j)*, riguardanti rispettivamente le piattaforme online (servizi di *hosting* che memorizzano e diffondono informazioni al pubblico) e i motori di ricerca online (servizi intermediari che consentono agli utenti di formulare domande per effettuare ricerche sulla base di un'interrogazione su qualsiasi tema).

[14] F. G'sell, *The Digital Services Act*, cit., 89.

[15] Cfr. L. D'Agostino, *Disinformazione e obblighi di* compliance *degli operatori del mercato digitale alla luce del nuovo* Digital Services Act*,* cit., par. 1 ed E. Birritteri, *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di* compliance *e dei poteri di autonormazione degli operatori*, cit., par. 1.

funzione di *compliance* dedicata[16], con lo scopo di colpire la propagazione di contenuti illegali e contrastare – per quanto qui d'interesse – anche la disinformazione online.
Del pari, il DSA tratteggia una complessa "*governance* pubblica" per l'efficace supervisione e attuazione della disciplina: l'articolazione dei poteri nel regolamento segue uno schema tendenzialmente decentrato che è stato definito come «rete regolatoria condivisa», in cui le diverse autorità coinvolte in ambito nazionale e la Commissione europea – senza dimenticare il livello "intermedio" rappresentato dal Comitato europeo per i servizi digitali – operano in collaborazione, riservandosi comunque agli Stati membri un ruolo di primo piano, pur nel contesto di un *framework* normativo armonizzato[17].
È evidente che un assetto di regole di tale portata sarebbe tuttavia destinato a rimanere ineffettivo ove non accompagnato da un puntuale e credibile meccanismo di implementazione che, nel caso di specie, è tratteggiato nel denso Capo IV del regolamento, dedicato appunto all'attuazione, alla cooperazione, alle sanzioni e all'esecuzione del DSA, oggetto della presente sezione della ricerca.
È questo uno degli ambiti di intervento del regolamento di sicuro interesse per il penalista, intercettando tra l'altro la questione dello spazio riservato – nella tutela sia dei diritti degli utenti di servizi digitali, sia delle funzioni delle autorità di *enforcement* coinvolte – alla risposta sanzionatoria, la quale – pur non ricorrendosi qui al diritto criminale – presenta non trascurabili connotati di afflittività.
Con l'obiettivo di offrire una panoramica dell'architettura dei poteri nel DSA avuto riguardo al versante pubblico e del riparto tra livello nazionale ed europeo (par. 2), il contributo ripercorre la progressione dell'articolato – ispirato a una logica, per così dire, "ascendente" –, come segue: si muove dalle competenze attribuite alle autorità dei singoli Stati membri e particolarmente ai coordinatori dei servizi digitali in relazione alla supervisione ed esecuzione del regolamento (par. 3); si passa a esaminare la disciplina in tema di assistenza reciproca e cooperazione transfrontaliera (par. 4) e le funzioni del Comitato europeo per i servizi digitali (par. 5); si analizza, poi, il ruolo da protagonista della Commissione europea nei rapporti con le piattaforme online e i motori di ricerca online di dimensioni molto grandi (par. 6); si conclude con alcune considerazioni sui caratteri di fondo delle scelte regolatorie del legislatore europeo in punto di *enforcement* del DSA (par. 7).

2. La distribuzione dei poteri di *enforcement* tra la Commissione europea e gli Stati membri

Dalla lettura delle previsioni del Capo IV emerge come dell'*enforcement* pubblico del DSA siano titolari sia gli Stati membri – in particolare, attraverso la designazione di un'autorità nazionale di regolamentazione competente, il coordinatore dei servizi di-

[16] Su cui, in dettaglio, v. E. Birritteri, *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di* compliance *e dei poteri di autonormazione degli operatori*, cit., par. 4.

[17] L. Torchia, *I poteri di vigilanza*, cit., 1111.

gitali[18] –, sia la Commissione europea.

Nel quadro di una «stretta cooperazione» tra livello nazionale ed europeo, l'art. 56 del regolamento traccia una *summa divisio* tra quanto è di esclusiva pertinenza degli Stati membri – ossia, in termini generali, l'esercizio dei poteri di vigilanza e applicazione del DSA, sulla base del criterio del luogo di stabilimento principale del *provider* di servizi intermediari, fatto salvo quanto subito si dirà[19] – e gli ambiti di intervento riservati alla sola Commissione – nello specifico, la supervisione sul rispetto degli obblighi più stringenti di cui si è fatta menzione (Capo III, sezione 5, artt. 33-43 DSA)[20] imposti ai fornitori di piattaforme online di dimensioni molto grandi (c.d. *Very Large Online Platforms – VLOPs*) e ai motori di ricerca online di dimensioni molto grandi (c.d. *Very Large Online Search Engines – VLOSEs*)[21].

Per tutte le altre norme applicabili alle «*large companies*» diverse da quelle appena citate si stabilisce, invece, una "competenza concorrente" tra Commissione e Stati membri (art. 56, par. 3, DSA), ma va sottolineato che l'attivarsi delle autorità nazionali del luogo di stabilimento è subordinato al fatto che la Commissione non abbia avviato procedimenti per la stessa infrazione (così il par. 4 del medesimo articolo). Ben si comprende, quindi, come il legislatore europeo abbia voluto comunque attribuire alla Commissione il primato per la trattazione e gestione delle vicende in cui sono coinvolti gli operatori di più grande dimensione/importanza: ciò risponderebbe alla logica di evitare quei problemi di *enforcement* sperimentati, ad esempio, nel contesto del GDPR[22] – ove, in ragione del *country-of-origin principle*, la competenza è di fatto nelle mani dell'autorità irlandese, avendo molte grandi aziende sede in tale Paese[23] –, sul presupposto di una maggior "resilienza" della Commissione alle dinamiche di *regulatory capture*[24].

La suddivisione di cui si è detto è valevole anche per l'ipotesi in cui un fornitore di servizi intermediari non abbia uno stabilimento nell'Unione: esso ricadrà dunque nella competenza dello Stato membro in cui risiede o è stabilito il suo rappresentante legale – che i *provider* in questione, se offrono servizi nell'Unione, possono nominare a norma dell'art. 13 DSA[25] – o in quella della Commissione, sulla base delle regole

[18] *Infra* par. 3.

[19] Il riparto di competenze tra Stati membri e Commissione è infatti ulteriormente precisato ai par. 2, 3 e 4 dell'art. 56 DSA.

[20] Per una analisi di tali disposizioni, v. V. Colarocco - M. Cogode, *Gli obblighi applicabili a piattaforme* online *di dimensioni molto grandi (Artt. 33-43 – Capo III, Sezione 5)*, in *Diritto di internet*, 1, 2023, 27 ss.

[21] Per le relative definizioni, v. *supra*, nt. 13.

[22] GDPR – regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE. Sull'effettiva capacità di *enforcement* dell'autorità irlandese v. la ricostruzione di M. Murgia - J. Espinoza, *Ireland is 'Worst Bottleneck' for Enforcing EU Data Privacy Law*, in *irishtimes.com*, 13 settembre 2021.

[23] F. G'sell, *The Digital Services Act*, cit., 106.

[24] I. Buri, *A Regulator Caught Between Conflicting Policy Objectives. Reflections on the European Commission's Role as DSA Enforcer*, in J. Van Hoboken e altri (a cura di), *Putting the Digital Services Act into Practice*, cit., 79; per alcune considerazioni sul punto, v. anche *infra* par. 7.

[25] L'art. 13, par. 1, DSA prescrive che i prestatori di servizi intermediari che non sono stabiliti nell'Unione ma che ivi offrono servizi «possono designare per iscritto una persona fisica o giuridica che funga da loro rappresentante legale in uno degli Stati membri in cui offrono i propri servizi».

appena delineate.
In mancanza della nomina di un rappresentante legale da parte del fornitore, tutti gli Stati membri, e la Commissione per i *provider* di *VLOPs* e *VLOSEs*, dispongono dei poteri di vigilanza e applicazione del regolamento, come chiarito dall'art. 56, par. 7, DSA. Per evitare sovrapposizioni e il rischio di duplicazioni procedimentali e sanzionatorie, tale previsione stabilisce che in queste circostanze, ove un coordinatore dei servizi digitali intenda procedere, sarà tenuto a informare tutti gli altri coordinatori nazionali e la Commissione, e lo stesso dovrà fare quest'ultima nell'ipotesi inversa.
Un meccanismo così congegnato appare in grado, in principio, di inibire l'avvio di plurimi *proceeding* per la medesima violazione, ciò che – unitamente agli obblighi di comunicazione e notifica incombenti, a seconda dei casi, sulle autorità nazionali e sulla Commissione per i procedimenti rispettivamente avviati[26] – parrebbe scongiurare potenziali casi di *bis in idem*[27].

3. Il livello nazionale. I coordinatori dei servizi digitali degli Stati membri: uno sguardo d'insieme

Come si accennava, il DSA prevede, all'art. 49, che gli Stati membri designino al loro interno una o più autorità incaricate della vigilanza dei fornitori di servizi intermediari e dell'esecuzione del regolamento («autorità competenti»). Ciascuno Stato individua, altresì, una delle suddette autorità quale *coordinatore dei servizi digitali*, che risulterà responsabile, a livello nazionale, «di tutte le questioni relative alla vigilanza e all'applicazione» del DSA, salvo che determinati compiti o settori non risultino attribuiti ad altre autorità competenti – cosa assai probabile essendo il DSA un regolamento orizzontale, che interessa diversi ambiti[28].
Per evitare il rischio di una frammentazione dei compiti[29], si prevede in ogni caso che sia il coordinatore dei servizi digitali ad assicurare l'efficace e coerente applicazione del DSA e a occuparsi, appunto, del coordinamento tra le eventuali autorità domestiche competenti. È dunque plausibile (e anzi, secondo alcuni commentatori, preferibile)[30] che gli Stati membri si muovano nella direzione di designare tali soggetti tra autorità esistenti e con esperienza nei settori vigilati – in Italia, ad esempio, candidature sono state avanzate dall'Autorità per le garanzie nelle comunicazioni e dal Garante per la

[26] V. in particolare *infra* nei paragrafi che seguono.

[27] In senso analogo I. Castellucci - F. Coppola, *Il sistema sanzionatorio decentrato del DSA: dinamica dell'apparato istituzionale*, in *Diritto di internet*, 1, 2023, 51 e 53. Manifesta invece qualche perplessità in relazione al fatto che il sistema delineato dal legislatore europeo sia in grado di «assicurare il rispetto del divieto di *bis in idem* sovranazionale» S. Braschi, *Il nuovo Regolamento sui servizi digitali: quale futuro per la responsabilità degli Internet Service Provider?*, in *Diritto penale e processo,* 3, 2023, 377.

[28] Sottolineano questo aspetto M. Husovec - I. Roche Laguna, *Digital Services Act: A Short Primer*, in *ssrn.com,* 2. Il contributo è in corso di pubblicazione in M. Husovec - I. Roche Laguna, *Principles of the Digital Services Act*, Oxford, 2023.

[29] Come osservato da L. Torchia, *I poteri di vigilanza*, cit., 1109.

[30] E. M. Tripodi, *Le Autorità competenti, i Coordinatori nazionali dei servizi digitali e il Comitato europeo per i servizi digitali. Brevi note*, in *Diritto di internet*, 1, 2023, 62.

protezione dei dati personali –, dando luogo a una sorta di «competizione» per l'attribuzione del ruolo di coordinatore[31].

I coordinatori sono tenuti ad agire in modo imparziale, trasparente e tempestivo, rendendosi a tal fine necessario che ciascuno Stato metta a disposizione adeguate risorse tecniche, finanziarie e umane e assicuri, del pari, sufficiente autonomia gestionale in relazione al bilancio – elemento questo indispensabile a preservare la piena indipendenza di tali soggetti, chiamati a operare al riparo da influenze esterne e senza richiedere o comunque ricevere istruzioni da parte di altre autorità pubbliche o da privati (art. 50 DSA).

Tra i profili più interessanti della disciplina in analisi si annoverano quelli riguardanti l'articolazione dei poteri d'indagine, esecuzione e sanzione previsti in capo ai coordinatori dei servizi digitali nei confronti dei *provider* che ricadono nella competenza del loro Stato membro[32].

Più precisamente, l'art. 51 DSA distingue e dettaglia le attività rientranti nel campo dei poteri d'indagine (par. 1) e quelle afferenti ai poteri d'esecuzione e sanzione (par. 2), prevedendo infine la possibilità, in via residuale e solo ove l'espletamento degli altri poteri non abbia sortito effetti, di ricorrere a misure ulteriori a carattere "ingiunzionale/inibitorio" (ivi inclusa quella delle restrizioni all'accesso) (par. 3)[33]. Si richiede che tutte le predette misure adottate dai coordinatori nell'esercizio di tali poteri siano – secondo la consueta formula – effettive, dissuasive e proporzionate[34], avuto riguardo alla natura, gravità, reiterazione e durata della violazione cui si riferiscono, e altresì, ove opportuno, alla capacità economica, tecnica e operativa del fornitore di servizi intermediari interessato (par. 5).

Osservando più da vicino il contenuto dei poteri dei coordinatori nazionali, in sede di *indagine* (art. 51, par. 1) questi possono imporre ai *provider* di fornire, senza indebito ritardo, informazioni relative a una presunta violazione del regolamento (lett. *a*); essi possono, altresì, effettuare ispezioni presso i locali utilizzati da tali fornitori «al fine di esaminare, sequestrare, prendere o ottenere copie di informazioni relative a una presunta violazione in qualsiasi forma», nonché chiedere a un'autorità giudiziaria nazionale di ordinare ispezioni, o a altre autorità pubbliche di procedervi (lett. *b*); da ultimo, i coordinatori dei servizi digitali possono domandare spiegazioni a qualsiasi membro del personale o rappresentante dei suddetti fornitori in merito a presunte violazioni e registrarne le risposte (lett. *c*).

I poteri d'indagine *sub* lett. *a*) e lett. *b)* possono, peraltro, attingere anche *altre perso-*

[31] Così G. Buttarelli, *La regolazione delle piattaforme digitali*, cit., 123. Per l'Italia la scelta è infine ricaduta sull'Autorità per le garanzie nelle comunicazioni (AGCOM), che è stata di recente designata quale coordinatore dei servizi digitali ai sensi dell'art. 15, d.l. 15 settembre 2023, n. 123. Si prevede, peraltro, che l'Autorità garante della concorrenza e del mercato, il Garante per la protezione dei dati personali e «ogni altra Autorità nazionale competente» assicurino la propria collaborazione, i cui aspetti applicativi e procedimentali potranno essere disciplinati mediante protocolli di intesa.

[32] Con le precisazioni di cui subito si dirà rispetto anche ad altri soggetti che possono essere attinti dall'esercizio dei poteri in discorso.

[33] Si prevede che poteri di cui ai par. 1, 2 e 3 lascino impregiudicata la sezione 3, relativa alla disciplina del Comitato europeo per i servizi digitali (cfr. art. 51, par. 4, DSA).

[34] Sulle tecniche di recepimento di tale clausola nel diritto interno v., per tutti, A. Gullo, *Deflazione e obblighi di penalizzazione di fonte UE*, in *Diritto penale contemporaneo*, 10 febbraio 2016.

ne che agiscano «per fini connessi alla propria attività commerciale, imprenditoriale, artigianale o professionale» e che possano «ragionevolmente essere a conoscenza di informazioni» in merito a una presunta violazione del DSA, ivi incluse le organizzazioni che effettuano le revisioni indipendenti *ex* artt. 37[35] e 75, par. 2 (nell'ambito della vigilanza rafforzata)[36] per i *provider* di piattaforme online e i motori di ricerca online di dimensioni molto grandi.

Rispetto ai poteri di *esecuzione* di cui all'art. 51, par. 2, DSA, occorre invece distinguere, dal momento che taluni si indirizzano unicamente alle piattaforme, mentre altri – legati all'*enforcement* delle sanzioni imposte dai coordinatori nazionali, di cui si dirà tra un momento – possono riguardare anche le altre persone menzionate nel par. 1.

Sul primo versante, vengono in rilievo il potere dei coordinatori di accettare gli impegni offerti dai *provider* in relazione alla loro conformità al regolamento e di rendere detti impegni vincolanti[37] (lett. *a*), nonché quelli – esercitabili direttamente o facendo richiesta a un'autorità giudiziaria statale – di ordinare la cessazione delle violazioni e, se opportuno, imporre misure correttive proporzionate e necessarie a tal fine (lett. *b*), e di adottare misure provvisorie per evitare il rischio di un danno grave (lett. *e*).

Quanto al secondo caso, le lett. *c)* e *d)* del par. 2 in discorso delineano, rispettivamente, il potere dei coordinatori dei servizi digitali – anche per il tramite di un'autorità giudiziaria nazionale – di imporre *sanzioni pecuniarie* per l'inosservanza del regolamento (dunque, anche con riferimento all'emissione degli ordini di indagine di cui al par. 1), nonché *penalità di mora* volte a garantire il rispetto di un ordine di cessazione delle violazioni di cui alla *lett. b)* o di uno dei, già ricordati, ordini di indagine. Trattasi di poteri che possono essere esercitati nei confronti non solo del *provider*, ma, come si è detto, anche di altre persone «in caso di mancato rispetto di uno qualsiasi degli ordini emessi nei loro confronti», previa informativa «in tempo utile» in relazione agli ordini in parola (compresi termine applicabile, sanzioni per l'inottemperanza, possibilità di ricorso). Le sanzioni, pertanto, non attengono qui *stricto sensu* a violazioni degli obblighi del DSA – i quali ricadono, in effetti, sui fornitori di servizi intermediari – ma presidiano piuttosto, attraverso l'impiego della tecnica ingiunzionale[38], l'inosservanza da parte di altri soggetti degli ordini impartiti dal coordinatore nazionale – ad esempio, quello di consentire un'ispezione o di fornire informazioni.

Il par. 3 dell'art. 51 DSA prevede, infine, il potere dei coordinatori dei servizi digitali di adottare misure ulteriori nei riguardi dei *provider* a condizioni molto stringenti – sostanzialmente quale *ultima ratio* – laddove tutti gli altri poteri *ex* art. 51 siano stati esauriti e la violazione non sia cessata, non vi sia stato posto rimedio o prosegua e causi

---

[35] V. al riguardo E. Birritteri, *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di* compliance *e dei poteri di autonormazione degli operatori,* cit., par. 4.4.

[36] *Infra* par. 6.1.

[37] Sul medesimo tema nel contesto dell'attività della Commissione v. *infra*, par. 6.1.

[38] Su tale tecnica sanzionatoria v. già C. Pedrazzi, *Odierne esigenze economiche e nuove fattispecie penali*, in *Rivista italiana di diritto e procedura penale*, 4, 1975, 1099 ss. L'utilizzo di tale tecnica è stato poi promosso in dottrina soprattutto nei contesti di incertezza scientifica: v. di recente, anche per ulteriori riferimenti bibliografici, E. Birritteri, *Salute pubblica, affidamento dei consumatori e diritto penale. Limiti e prospettive di tutela nel settore alimentare tra individuo ed ente collettivo*, Torino, 2022, 270 ss.

un danno grave, non evitabile neppure attraverso l'esercizio di altri poteri a livello unionale o nazionale.

Nell'alveo di queste misure rientrano: l'imposizione all'organo di gestione di tali fornitori di esaminare la situazione senza ritardo, di adottare e presentare un piano di azione che definisca le misure necessarie alla cessazione della violazione, di provvedere affinché il *provider* le adotti e di riferire su di esse (lett. a); la richiesta all'autorità giudiziaria competente dello Stato membro di ordinare la restrizione temporanea dell'accesso al servizio interessato dalla violazione da parte dei destinatari o, solo se ciò non sia fattibile tecnicamente, la restrizione dell'accesso all'interfaccia online interessata dalla violazione (lett. b).

Come si è anticipato, la richiesta di restrizione all'accesso, quale misura invasiva e incidente su diritti fondamentali, è attivabile solo a fronte di violazioni di rilevante gravità e la relativa procedura è accompagnata da particolari garanzie. Il coordinatore dei servizi digitali può, invero, procedere rivolgendosi all'autorità giudiziaria nazionale solo ove ritenga che un fornitore di servizi intermediari non si sia conformato in modo sufficiente agli obblighi appena descritti *sub* art. 51, par. 3, lett. a) DSA, e che alla violazione non si sia rimediato e che essa causi un danno grave e integri un reato grave che minacci la vita o la sicurezza delle persone.

Prima di inoltrare tale richiesta il coordinatore è tenuto a invitare le parti interessate a presentare osservazioni scritte, illustrando le misure individuate e identificando i destinatari delle stesse. La norma ribadisce che, quanto alla scelta, le misure debbono risultare «proporzionate alla natura, alla gravità, alla reiterazione e alla durata della violazione», senza limitare indebitamente l'accesso alle informazioni lecite da parte dei destinatari del servizio. Si prevede, poi, nell'ambito del procedimento giudiziario dinanzi all'autorità competente, la possibilità di partecipazione del *provider*, dei destinatari previsti e dei terzi che abbiano un interesse legittimo.

Le suddette restrizioni all'accesso sono disposte per un periodo di quattro settimane, passibili di proroga, entro il numero massimo stabilito, per ulteriori periodi della stessa durata, su ordine dell'autorità giudiziaria competente. L'art. 51, par. 3, DSA chiarisce inoltre un aspetto di rilievo, legato alla circostanza che il coordinatore dei servizi digitali può prorogare il periodo di restrizione unicamente se – considerati i diritti dei soggetti a vario titolo coinvolti – ricorrono, congiuntamente, due condizioni: ossia, che il fornitore di servizi intermediari non abbia adottato le misure necessarie alla cessazione della violazione e che la restrizione temporanea non limiti indebitamente l'accesso dei destinatari del servizio alle informazioni lecite (avuto riguardo al numero di destinatari interessati e all'esistenza di alternative adeguate e facilmente accessibili). Se tali condizioni persistono ma non è più possibile prorogare, il coordinatore potrà presentare una nuova richiesta di restrizione all'accesso all'autorità giudiziaria.

Va detto che sono stati avanzati dubbi in merito alla compatibilità di tale prescrizione con il principio di proporzionalità – ribadito, come visto, dallo stesso art. 51 DSA – nella parte in cui essa dispone una durata fissa, pari a quattro settimane, del periodo di restrizione e dei successivi periodi di proroga, senza dare al giudice la possibilità di una modulazione parametrata sulle effettive esigenze poste dal caso concreto; a ciò si aggiungono perplessità legate alla circostanza che il DSA non prenda posizione sul

numero massimo di rinnovi, che spetterà alla stessa autorità giudiziaria stabilire[39].
Da ultimo, l'art. 51 del DSA si premura di affidare agli Stati la definizione delle condizioni e le procedure specifiche per l'esercizio dei poteri qui descritti, secondo le garanzie previste dal diritto nazionale, in conformità alla Carta di Nizza e al diritto dell'Unione, con particolare attenzione al rispetto della vita privata e al diritto di difesa.

3.1. *(Segue)*. I poteri sanzionatori degli Stati membri e gli strumenti di tutela dei destinatari del servizio

Venendo ora a esaminare l'apparato punitivo tratteggiato, nel DSA, all'art. 52, deve in primo luogo evidenziarsi come il legislatore europeo si sia orientato nel senso di demandare agli Stati membri di stabilire norme relative alle sanzioni applicabili in caso di violazioni del regolamento da parte dei *provider* rientranti nella loro competenza, nonché di adottare ogni misura necessaria a assicurare l'implementazione del DSA e di notificare poi tali norme e misure alla Commissione, anche in sede di eventuali successive modifiche.
Ancora, la norma chiarisce che gli Stati membri sono chiamati ad assicurare una risposta sanzionatoria che presenti i connotati dell'effettività, proporzionalità e dissuasività (par. 2). Nondimeno, mancano indicazioni espresse sulla *natura* delle sanzioni – dovendosi in ogni caso ritenere che si tratti di sanzioni amministrative[40] – mentre se ne definisce la tipologia – essenzialmente, di carattere pecuniario – e si prevede altresì un tetto massimo per gli importi di tali «penalties».
L'art. 52 DSA, nella specie, attribuisce ai coordinatori nazionali la prerogativa di irrogare sanzioni pecuniarie (*fine*) e penalità di mora (*periodic penalty payment*).
In particolare, quanto alla prima categoria, ai sensi del par. 3, si dovrà assicurare che l'importo massimo di tali sanzioni per i casi di inosservanza di un obbligo stabilito dal DSA sia pari al 6% del fatturato annuo mondiale del fornitore di servizi intermediari interessato, considerando l'esercizio finanziario precedente.
Nel caso, invece, di sanzione pecuniaria per la comunicazione di informazioni inesatte, incomplete o fuorvianti, di mancata risposta o rettifica di tali informazioni e di inosservanza dell'obbligo di sottoporsi a un'ispezione, gli Stati membri dovranno provvedere affinché l'importo massimo sia pari all'1 % del reddito annuo o del fatturato mondiale del fornitore dei servizi intermediari o della persona interessati, sempre nell'esercizio finanziario precedente.
Si utilizza, sul punto, una tecnica diversa da quella di cui all'art. 83 GDPR in materia di *privacy*, ove, a seconda del tipo di violazione, si fissa un massimo pari a 10 o 20 milioni

[39] V. le argomentazioni di I. Castellucci - F. Coppola, *Il sistema sanzionatorio decentrato del DSA*, cit., 54.

[40] Per rimanere nel campo dei regolamenti, cfr. art. 83 GDPR, dove si parla espressamente di sanzioni *amministrative* pecuniarie (corsivo aggiunto). Con riferimento all'ordinamento italiano, v. ora quanto previsto dall'art. 15, co. 4, lett. *b)*, d.l. 123/2023, ove si chiarisce che l'Autorità, nell'esercizio dei poteri di cui al combinato disposto degli artt. 51e 52 DSA, irroga «in base a principi di proporzionalità, adeguatezza e rispetto del contraddittorio, secondo le procedure stabilite con proprio regolamento, sanzioni amministrative pecuniarie», richiamandosi la l. 689/1981 per escludere l'applicabilità del beneficio del pagamento in misura ridotta ivi previsto all'art. 16.

di euro o, per le imprese, pari al 2% o 4% del fatturato mondiale annuo, solo però se superiore ai predetti importi; a differenza del DSA, quindi, il fatturato rappresenta un criterio alternativo[41].

Il tetto dell'altra *penalty* prevista dal par. 4 dell'art. 52 DSA, ossia la penalità di mora – che può essere imposta, come anticipato, per assicurare il rispetto di un ordine di cessazione delle violazioni o di uno degli ordini di indagine[42] – non può superare il 5% del fatturato – in questo caso – giornaliero medio mondiale o del reddito del fornitore di servizi intermediari interessato nel precedente esercizio finanziario, calcolato a decorrere dalla data specificata nella decisione.

Appare poi di interesse fare alcuni cenni ai mezzi di tutela dell'utente delineati specificamente nell'ambito della disciplina delle prerogative del coordinatore dei servizi digitali, subito a seguire le previsioni in materia di poteri e sanzioni sin qui esaminate.

Preliminarmente, è bene ricordare che il DSA prevede, in termini generali, diversi possibili rimedi, sia di tipo *interno* alle piattaforme – si fa riferimento in particolare ai sistemi di gestione dei reclami che gli stessi operatori sono tenuti a implementare, *ex* art. 20 DSA –, sia di tipo *esterno*, compresa la possibilità di «scegliere qualunque organismo di risoluzione extragiudiziale delle controversie»[43] certificato dal coordinatore nazionale, anche per definire i *complaint* «che non è stato possibile risolvere mediante il sistema interno di gestione dei reclami» (art. 21, par. 1, DSA)[44].

Rispetto a tale opzione, poiché l'art. 21, par. 2, DSA stabilisce che l'organismo in questione non ha comunque il potere di imporre alle parti una risoluzione vincolante della controversia, in caso di perdurante disaccordo rimane impregiudicato il diritto degli utenti di adire un organo giurisdizionale conformemente al diritto applicabile, ad esempio per ottenere la rimozione di contenuti online. Qui viene in rilievo anche la disposizione – inserita nella sezione 1 del Capo IV in commento, dedicata ai coordinatori nazionali – secondo cui i destinatari del servizio possono chiedere un risarcimento ai fornitori di servizi intermediari, conformemente al diritto dell'Unione e a quello nazionale, in relazione a danni o perdite subiti a seguito di una violazione degli obblighi stabiliti dal regolamento (art. 54 DSA).

Tra i rimedi relativi all'«*access to justice outside of platforms*»[45], il DSA introduce la possibilità, per i destinatari del servizio – oltre che per i soggetti incaricati di esercitare, per conto di costoro, i diritti conferiti dal DSA (ad esempio organismi, organizzazioni,

[41] Per un commento alla norma v. S. Aterno, Sub *art. 83*, in G.M. Riccio - G. Scorza - E. Belisario (a cura di), *GDPR e normativa* privacy. *Commentario*, Milano, 2022, 734 ss. Una puntuale analisi, in chiave critica, della tecnica adoperata dal legislatore europeo per la comminatoria delle sanzioni nel GDPR e delle correlate scelte operate, sul punto, in ambito domestico, è svolta da L. D'Agostino, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101*, in *Archivio penale web*, 1, 2019, 21 s.

[42] *Supra*, par. 3.

[43] V. in argomento A.M. Felicetti, *La risoluzione extragiudiziale delle dispute nei mercati digitali: alcune novità dall'Europa*, in *Rivista trimestrale di diritto e procedura civile*, 1, 2023, 197 ss.

[44] Su tali previsioni, si rinvia a E. Birritteri, *Contrasto alla disinformazione,* Digital Services Act *e attività di* private enforcement*: fondamento, contenuti e limiti degli obblighi di* compliance *e dei poteri di autonormazione degli operatori,* cit. (parr. 3.1 e 3.2).

[45] Su cui v. P. Ortolani, *If You Build it, They Will Come. The DSA "Procedure Before Substance" Approach*, in J. Van Hoboken e altri (a cura di), *Putting the Digital Services Act into Practice*, cit., 158 ss.

associazioni) – di proporre al coordinatore dei servizi digitali dello Stato in cui essi sono situati o stabiliti dei reclami (*complaint*) vertenti su violazioni del regolamento nei confronti dei fornitori di servizi intermediari (art. 53 DSA).
La procedura prevede che il coordinatore ricevente debba provvedere a valutare il reclamo e, se del caso, trasmetterlo al coordinatore dei servizi digitali del luogo di stabilimento, eventualmente corredato da un parere; inoltre, nell'ambito del suo ruolo di coordinamento, se reputa che il reclamo rientri nella responsabilità di un'altra autorità competente nel suo stesso Stato, il coordinatore ricevente lo trasmette a quest'ultima. Entrambi le parti conservano, in tali circostanze, il diritto di essere ascoltati e di ricevere informazioni sullo stato del reclamo.

4. La disciplina in tema di assistenza reciproca con la Commissione europea e cooperazione transfrontaliera dei coordinatori nazionali

La sezione 2 del Capo IV delinea una puntuale disciplina – nel quadro del riparto di competenze tra livello nazionale e europeo di cui si parlato[46] – in materia di assistenza reciproca (art. 57 DSA), cooperazione transfrontaliera tra coordinatori di servizi digitali e deferimento alla Commissione (artt. 58-59 DSA), nonché indagini comuni (art. 60 DSA).
Emerge qui con particolare nitore il complesso di tipo "reticolare" di cui si è detto: l'operato dei diversi attori, nell'ottica di mutua collaborazione, è scandito da tempistiche predeterminate e alquanto serrate; appare inoltre chiaro come uno degli obiettivi di fondo di tali previsioni sia quello di evitare l'inerzia delle autorità coinvolte, disponendo che in caso di mancato rispetto dei termini fissati, soccorrano meccanismi certi per il superamento della stasi decisionale in merito a una presunta violazione.
La prima norma rilevante attiene all'assistenza reciproca tra i coordinatori dei servizi digitali e la Commissione, in cui rientrano – nell'ottica di una coerente ed efficiente applicazione del DSA – lo scambio di informazioni e il dovere, in capo al coordinatore del luogo di stabilimento, di informare tutti i coordinatori dei servizi digitali del luogo di destinazione, il Comitato europeo per i servizi digitali e la Commissione in caso di avvio di un'indagine e rispetto all'intenzione di adottare una decisione definitiva nei confronti di uno specifico *provider* di servizi intermediari (art. 57, par. 1, DSA).
La collaborazione si estrinseca anche attraverso la possibilità che il coordinatore del luogo di stabilimento richieda informazioni – o richieda di esercitare i poteri di indagine ai sensi dell'art. 51, par. 1, DSA – ad altri coordinatori dei servizi digitali, i quali sono tenuti a soddisfare la richiesta «senza indebito ritardo» e comunque entro due mesi dal suo ricevimento. Se non è possibile dare a essa seguito – e le ragioni normativamente ammesse sono limitate ai casi di richiesta non sia sufficientemente specificata, motivata o proporzionata alla luce delle finalità dell'indagine, di mancato possesso delle informazioni e di impossibilità di soddisfare detta richiesta senza violare il diritto dell'Unione o nazionale –, il coordinatore ricevente dovrà giustificare il rifiuto, presen-

[46] *Supra*, par. 2.

tando, entro il medesimo termine, una risposta motivata.
Proseguendo, la previsione in tema di cooperazione transfrontaliera tra i coordinatori dei servizi digitali, *ex* art. 58 DSA, si apre con una clausola di salvaguardia che impedisce ai coordinatori nazionali di attivarsi nel caso in cui la Commissione abbia avviato un'indagine per la stessa presunta violazione.
Ove così non sia, il coordinatore dei servizi digitali del luogo di destinazione che sospetti una violazione del regolamento con possibili ripercussioni negative sui destinatari del servizio nel proprio Stato membro, perpetrata da un fornitore di servizi intermediari, può chiedere al coordinatore del luogo di stabilimento di valutare la questione e adottare le misure di indagine ed *enforcement* necessarie (par.1). La medesima procedura può essere messa in moto dal Comitato su richiesta di almeno tre coordinatori dei servizi digitali del luogo di destinazione nelle medesime circostanze (par. 2)[47].
Si prescrive che il coordinatore dei servizi digitali del luogo di stabilimento debba tenere «nella massima considerazione» tali richieste, anche domandando informazioni supplementari al coordinatore richiedente o al Comitato, secondo la procedura dell'art. 57 DSA o, in alternativa, avviando un'indagine congiunta ai sensi dell'art. 60, par. 1, DSA; in ogni caso, è tenuto a comunicare la sua valutazione sulla presunta violazione, unitamente a una spiegazione delle eventuali misure di indagine o di esecuzione adottate o previste, entro due mesi dal ricevimento della richiesta.
Per i casi, sostanzialmente, di mancata valutazione o di disaccordo sul merito delle scelte proposte, la normativa introduce anche una procedura di *referral* da parte del Comitato europeo per i servizi digitali alla Commissione (art. 59 DSA), volta a evitare il rischio di inazione o l'adozione di misure insoddisfacenti da parte delle autorità nazionali. La Commissione è a sua volta chiamata a valutare la questione entro due mesi dal deferimento, ma se ritiene che le misure già adottate siano insufficienti o incompatibili con il DSA, può fornire un parere, richiedendo al coordinatore dei servizi digitali del luogo di stabilimento di riesaminare il caso[48].
Merita un cenno anche la disciplina delle indagini comuni che possono essere avviate e dirette dal coordinatore dei servizi digitali del luogo di stabilimento – di propria iniziativa o dietro raccomandazione del Comitato, su richiesta di almeno tre coordinatori – con la partecipazione di altri coordinatori interessati, laddove venga in rilievo una violazione del DSA con impatto in più Stati membri.
I coordinatori dei servizi digitali partecipanti cooperano in buona fede e, peraltro, qualsiasi coordinatore che dimostri di avere un interesse legittimo alla partecipazione può fare richiesta; ai coordinatori dei servizi digitali del luogo di destinazione si riconosce il diritto di esercitare i loro poteri di indagine nei confronti dei fornitori di

[47] Ai sensi dell'art. 58, par. 3, DSA, le richieste in questione debbono essere motivate e specifiche almeno rispetto al punto di contatto del fornitore di servizi intermediari interessato ai sensi dell'art. 11 DSA, alla descrizione dei fatti rilevanti, delle disposizioni del DSA interessate, dei motivi di sospetto e della descrizione degli effetti negativi della presunta violazione, nonché a qualsiasi altra informazione che il coordinatore richiedente o il Comitato ritenga pertinenti, compresi suggerimenti per l'adozione di specifiche misure di indagine o di esecuzione.

[48] L'art. 59, par. 3, DSA precisa che «il coordinatore dei servizi digitali del luogo di stabilimento adotta le misure di indagine o di esecuzione necessarie […] tenendo nella massima considerazione il parere e la richiesta di riesame della Commissione», dovendo poi fornire informazioni in merito alle misure adottate entro due mesi dalla richiesta di riesame.

servizi intermediari interessati per ciò che concerne le informazioni e i locali situati nel loro territorio.

Anche in sede di indagini congiunte, è poi fatta salva, a specifiche condizioni, la possibilità di deferimento alla Commissione a cura del Comitato[49].

A garanzia della certezza dei tempi procedimentali è stabilito un termine di tre mesi per la conclusione dell'indagine – decorrenti, salvo diverso accordo tra i partecipanti, dall'avvio della stessa – e, non oltre un mese da tale scadenza, il coordinatore dei servizi digitali che ha promosso l'indagine dovrà comunicare a tutti i coordinatori dei servizi digitali, alla Commissione e al Comitato la sua posizione preliminare sulla presunta violazione, con la quale si potranno disporre anche misure di esecuzione.

5. Il raccordo istituzionale tra Stati membri e Commissione europea: il Comitato europeo per i servizi digitali

L'architettura del DSA prevede l'istituzione del – più volte menzionato – Comitato europeo per i servizi digitali[50], soggetto in qualche misura "intermedio" tra il livello nazionale – rappresentato dalle autorità competenti con il ruolo chiave, come illustrato, assegnato ai coordinatori dei servizi digitali – e il livello europeo, che vede protagonista delle attività di *enforcement* destinate ai grandi *player* del mercato digitale la Commissione.

È possibile considerare il Comitato una realtà "a metà strada" nel riparto di competenze tra Stati membri e Commissione, dal momento che esso è composto, come subito si dirà, da coordinatori dei servizi digitali nazionali, ma è presieduto dalla Commissione: si tratta, quindi, del meccanismo istituzionalmente previsto per il raccordo, in tema di vigilanza sull'applicazione del regolamento, tra ambito nazionale ed europeo. Come si è osservato, simili organismi non costituiscono una novità nel panorama regolatorio dell'Unione: si pensi, nel contesto della protezione dei dati, allo *European Data Protection Board*[51].

I caratteri essenziali del Comitato, avuto riguardo agli obiettivi perseguiti, alla struttura e ai compiti, sono descritti nella sezione 3 del Capo IV del DSA (artt. 62-64 DSA). Più in particolare, il Comitato è un gruppo consultivo indipendente di coordinatori dei servizi digitali per la vigilanza sui *provider* di servizi intermediari, la cui *mission* è di contribuire all'applicazione coerente del regolamento e alla cooperazione efficace dei coordinatori nazionali e della Commissione, agli orientamenti e alle analisi della Commissione, dei coordinatori nazionali e di altre autorità competenti sulle questioni emergenti nel mercato interno nelle materie disciplinate dal DSA, nonché di assistere

[49] Ai sensi dell'art. 60, par. 3, DSA il Comitato può deferire la questione alla Commissione se: il coordinatore dei servizi digitali del luogo di stabilimento non abbia comunicato la sua posizione preliminare entro il termine previsto; se si trovi in sostanziale disaccordo con la posizione preliminare comunicata dal predetto coordinatore; se quest'ultimo abbia omesso di avviare prontamente l'indagine congiunta a seguito di raccomandazione del Comitato.

[50] Sul tema v. E. M. Tripodi, *Le Autorità competenti*, cit., 63 ss.

[51] Cfr. G. Buttarelli, *La regolazione delle piattaforme digitali*, cit., 123.

i coordinatori dei servizi digitali e la Commissione nella vigilanza sulle piattaforme online di dimensioni molto grandi (art. 61, par. 2, DSA).

Quanto alla sua composizione, si prevede la partecipazione di tutti i coordinatori dei servizi digitali degli Stati membri rappresentati da funzionari di alto livello[52]. Se tuttavia in ambito nazionale vi sono altre autorità competenti «investite di specifiche responsabilità operative per l'applicazione e l'esecuzione» del DSA insieme al coordinatore dei servizi digitali, esse possono partecipare al Comitato; è altresì ammessa la possibilità che altre, diverse autorità nazionali possano essere invitate alle riunioni, ove siano oggetto di discussione questioni per loro di rilievo.

Per evitare che il Comitato non possa attivarsi in ragione dell'inerzia degli Stati membri, è stabilito che la mancata designazione di uno o più coordinatori dei servizi digitali nazionali non impedisce a esso di svolgere i propri compiti (art. 62, par. 1, DSA).

Come si anticipava, è la Commissione a presiedere il Comitato e a convocarne le riunioni, fornendo anche il necessario sostegno amministrativo e analitico per lo svolgimento delle attività[53]. Alle riunioni del Comitato possono essere invitati esperti e osservatori e si prevede la possibilità di cooperazione con altre istituzioni e altri organi dell'Unione nonché con esperti esterni, e di consultazione delle parti interessate, assicurando che i risultati di dette attività siano resi disponibili per il pubblico.

Se, secondo le prescrizioni del DSA, al Comitato è richiesto di adottare una raccomandazione[54], esso deve mettere tale richiesta a disposizione degli altri coordinatori dei servizi digitali nazionali «immediatamente», avvalendosi del sistema di condivisione delle informazioni appositamente previsto dall'art. 85 DSA: si tratta, nella specie, di un sistema affidabile e sicuro che dovrà essere istituito e manutenuto dalla Commissione europea e che rappresenterà il canale ordinario per lo scambio di informazioni tra i coordinatori dei servizi digitali, la Commissione e il Comitato, i quali ne dovranno fare uso per tutte le comunicazioni sancite dal regolamento.

Con riferimento ai meccanismi di funzionamento del Comitato, ogni Stato membro dispone di un voto mentre la Commissione non ha diritto di voto, e gli atti del Comitato sono adottati a maggioranza semplice (art. 62, par. 3, DSA).

I compiti del Comitato sono delineati all'art. 63 DSA e ad alcuni di questi – data la natura "trasversale" di tale organismo – si è già fatto o si farà ancora riferimento: si tratta del supporto al coordinamento delle indagini congiunte di cui all'art 60 DSA[55]; dell'as-

[52] Osserva E.M. Tripodi, *Le Autorità competenti*, cit., 64 che «[d]el «gruppo» fanno parte funzionari di alto livello (uno per ogni coordinatore nazionale con «diritto di voto» mentre possono essere presenti anche altri rappresentanti per le autorità competenti, ovvero altre autorità nazionali), ma non il Presidente o il rappresentante del Coordinatore nazionale. Si tratta, pertanto di un consesso "tecnico" e non politico».

[53] Il funzionamento del Comitato sarà disciplinato da un regolamento interno, adottato previo accordo con la Commissione (art. 62, par. 7, DSA).

[54] Tra le raccomandazioni che il Comitato può proporre, si segnala quella prevista nel contesto della particolare procedura di risposta alle crisi *ex* art. 36 DSA, nell'ambito della quale la Commissione può imporre a uno o più fornitori di piattaforme online o di motori di ricerca online di dimensioni molto grandi di intraprendere azioni preventive, di mitigazione dei rischi e di *reporting* «quando circostanze eccezionali» comportino una minaccia grave «per la sicurezza pubblica o la salute pubblica nell'Unione o in parti significative di essa» (questa la definizione di "crisi" di cui all'art. 36, par. 2, DSA). In tali casi, il Comitato è tenuto a votare entro 48 ore dalla richiesta del suo presidente (art. 62, par. 3, DSA).

[55] V. *supra*, par. 4.

sistenza alle autorità competenti nell'analisi delle relazioni e dei risultati delle revisioni di *VLOPs* e *VLOSEs*[56]; della predisposizione di pareri, raccomandazioni o consulenze ai coordinatori dei servizi digitali nazionali; della consulenza alla Commissione in riferimento all'avvio di un procedimento a carico di *provider* di piattaforme online o motori di ricerca online di dimensioni molto grandi (art. 66 DSA)[57] e di adozione di pareri in relazione ai medesimi soggetti; della promozione dell'elaborazione e attuazione di norme, orientamenti, relazioni, modelli e codici di condotta europei in cooperazione con i pertinenti portatori di interessi, come previsto dal DSA, anche fornendo pareri o raccomandazioni su questioni connesse all'art. 44 DSA (in tema di sviluppo e attuazione di *voluntary standards*), nonché dell'individuazione di questioni emergenti in relazione alle materie disciplinate dal regolamento.

L'art. 63, par. 2, DSA chiarisce che per discostarsi da tali pareri, richieste o raccomandazioni del Comitato i coordinatori dei servizi digitali (e, se del caso, le altre autorità nazionali competenti) debbono giustificare la scelta, fornendo una spiegazione sulle indagini, le azioni e le misure che hanno attuato.

6. I poteri di *enforcement* della Commissione europea: un "interlocutore privilegiato" dei più grandi *player* del mercato digitale

Nella struttura di tipo ascendente – dal livello nazionale a quello europeo – che l'articolato del DSA pare delineare nel Capo qui in commento, la relativa sezione 4 è dedicata in larga parte all'analisi dei poteri della Commissione europea[58], soggetto che – come si è già posto in luce – assume importanza entrale nell'*enforcement* pubblico del DSA, con particolare riferimento alle piattaforme online e ai motori di ricerca online di dimensioni molto grandi.

L'analisi svolta ha già fatto emergere come l'operato della Commissione in tale contesto si orienti in una duplice direzione: in generale, come attività di *enforcement* concorrente rispetto a quella dei coordinatori nazionali in rapporto alle possibili violazioni del DSA da parte dei *player* di grandi dimensioni; e, particolarmente, come meccanismo esclusivo di risposta alla violazione, perpetrata da tali soggetti, degli obblighi specifici contenuti nella sezione 5 del Capo III.

Invero, la norma di apertura della sezione ora in esame puntualizza, nella cornice di un generale ruolo di promozione e sviluppo delle competenze e capacità dell'Unione *in subiecta materia* da parte della Commissione, che a questa spetta il coordinamento della valutazione delle questioni sistemiche ed emergenti in tutta l'Unione in relazione alle piattaforme online e ai motori di ricerca online di dimensioni molto grandi (art. 64, par.

[56] Si possono ad esempio richiamare le revisioni indipendenti *ex* artt. 37 e 75, par. 2, DSA già menzionate *supra*, par. 3.

[57] Su cui v. *infra*, par. 6.

[58] Per alcune considerazioni sul ruolo della Commissione nel contesto del DSA v. A. Contaldo, *Il DSA e le competenze della Commissione europea sulla stregua della procedura anticoncorrenziale e la scelta del* "ne bis in idem", in *Diritto di internet*, 1, 2023, 73 ss.

2, DSA). Ciò a ribadire – fatti salvi i predetti obblighi del Capo III, sezione 5 – che di tali categorie di destinatari possano, in principio, occuparsi anche i coordinatori nazionali, pur competendo il "coordinamento generale" alla Commissione.

Rispetto all'assetto dei poteri della Commissione nei confronti delle «*large platforms*», può osservarsi che essi ricalcano, per molti versi, quelli già visti rispetto ai coordinatori dei servizi digitali degli Stati membri[59]: anche qui vengono in considerazione poteri d'indagine, poteri di esecuzione e di imposizione di sanzioni ma – come si avrà modo di chiarire – da un lato, anche rispetto a tali poteri "comuni", le norme della sezione dedicata all'*enforcement* da parte della Commissione sono, sul piano dei contenuti, maggiormente dettagliate; dall'altro, si aggiungono strumenti peculiari, di cui solo la Commissione dispone, rivolti unicamente a *VLOPs* e *VLOSEs*.

All'art. 65 il regolamento si premura anzitutto di precisare che la Commissione può esercitare i poteri di indagine sia di propria iniziativa, sia su richiesta di un coordinatore nazionale[60], anche prima di avviare un formale procedimento, secondo i dettami dell'art. 66, par. 2, DSA.

L'*iter* di accertamento di eventuali violazioni di disposizioni del DSA da parte di *provider* di piattaforme online e motori di ricerca online di dimensioni molto grandi segue infatti precisi *step* procedurali: la Commissione, ove sospetti che la condotta di uno di tali soggetti importi una violazione, può avviare un procedimento in vista dell'adozione di una decisione di non conformità (art. 73 DSA) e dell'irrogazione di sanzioni pecuniarie (art. 74 DSA). A tal fine, essa ne dà notifica all'interessato e altresì al Comitato e a tutti i coordinatori dei servizi digitali (art. 66, par. 1, DSA), essendo questi ultimi tenuti a trasmettere, senza indebito ritardo, ogni rilevante informazione di cui siano in possesso.

All'apertura di un procedimento da parte della Commissione consegue l'esonero, per qualsiasi autorità competente, dall'esercizio dei propri poteri di vigilanza ed esecuzione stabiliti nel DSA[61], ferma restando la possibilità che la Commissione richieda il sostegno, singolo o congiunto, dei coordinatori dei servizi digitali interessati dalla presunta violazione[62], i quali dovranno cooperare «lealmente e tempestivamente» (art. 66, par.

[59] *Supra*, par. 3.

[60] Nella specie, ai sensi dell'art. 65, par. 2, DSA 2 ove un coordinatore dei servizi digitali abbia motivo di sospettare che un fornitore di una piattaforma online o di un motore di ricerca online di dimensioni molto grandi abbia violato le disposizioni del Capo III, sezione 5, o abbia violato sistematicamente una delle disposizioni del regolamento con gravi ripercussioni per i destinatari del servizio nel suo Stato membro, può presentare – attraverso il sistema di condivisione delle informazioni *ex* art. 85 – una richiesta alla Commissione affinché valuti la questione. La richiesta è «debitamente motivata» e specifica almeno il punto di contatto della *VLOP* o del *VLOSE*, una descrizione dei fatti rilevanti, delle disposizioni del DSA pertinenti e dei motivi per cui il coordinatore richiedente sospetti violazioni del regolamento, nonché qualsiasi altra informazione questi ritenga pertinente, comprese quelle raccolte di propria iniziativa (art. 65, par. 3, DSA).

[61] Il richiamo è all'art. 56, par. 4, DSA a mente del quale «[q]ualora la Commissione non abbia avviato procedimenti per la stessa infrazione, lo Stato membro in cui è situato lo stabilimento principale del fornitore di una piattaforma online di dimensioni molto grandi o di un motore di ricerca online di dimensioni molto grandi dispone di poteri di vigilanza e di applicazione degli obblighi di cui al presente regolamento diversi da quelli di cui al capo III, sezione 5, nei confronti di tali fornitori».

[62] I quali potranno a quel punto, conformemente alla richiesta, esercitare i loro poteri di indagine (art. 51, par. 1, DSA) nei confronti del *provider* della piattaforma online o del motore di ricerca online di dimensioni molto grandi riguardo alle informazioni e ai locali ubicati nel loro Stato membro (art. 66, par. 3, DSA).

3, DSA).

Come si anticipava, i poteri attivabili in sede d'indagine, funzionali allo svolgimento dei compiti assegnati alla Commissione, sono sostanzialmente analoghi a quelli attribuiti alle autorità nazionali e attengono alla richiesta di informazioni (art. 67 DSA), alle audizioni e raccolta di dichiarazioni (art. 68 DSA), all'effettuazione di ispezioni (art. 69 DSA), all'adozione di misure provvisorie (art. 70), alla possibilità che la Commissione renda gli impegni assunti dal *provider* vincolanti e ponga in essere le relative azioni di monitoraggio (artt. 71 e 72 DSA).

Per assicurare un "controllo incrociato" sull'operato della Commissione, si stabilisce in ogni caso che essa debba fornire al coordinatore dei servizi digitali del luogo di stabilimento e al Comitato europeo per i servizi digitali tutte le pertinenti informazioni sull'esercizio dei suddetti poteri, nonché le sue constatazioni preliminari, sulle quali il Comitato è chiamato a fornire un parere[63].

Soffermando l'attenzione sui profili caratterizzanti i poteri di cui la Commissione è titolare, anche nel raffronto con quelli delle autorità nazionali, possono essere sottolineati, in linea generale, alcuni aspetti.

Anzitutto, anche i poteri della Commissione si indirizzano tanto ai grandi *player* direttamente, quanto a «qualsiasi altra persona fisica o giuridica che agisca per fini connessi alla propria attività commerciale, imprenditoriale, artigianale o professionale e che possa ragionevolmente essere a conoscenza di informazioni relative alla presunta violazione, comprese le organizzazioni che effettuano le revisioni indipendenti *ex* artt. 37 e 75, par. 2», al riguardo ricalcandosi testualmente l'art. 51 DSA[64] con riferimento a quanto disposto per i coordinatori nazionali.

In secondo luogo, ove è previsto che tali poteri siano, o possano essere, esercitati mediante decisione (come per le richieste di informazioni o le ispezioni), la Commissione è tenuta a specificare, tra l'altro, lo scopo della richiesta, i tempi, le sanzioni pecuniarie e le penalità di mora irrogabili, indicando il diritto dei soggetti incisi di chiedere il riesame della decisione alla Corte di giustizia dell'Unione europea.

Inoltre, le norme in tema di poteri d'indagine della Commissione paiono improntate ad assicurare – forse anche in modo ancora più puntuale rispetto alle omologhe disposizioni riguardanti i coordinatori nazionali – un costante flusso di comunicazione e scambio reciproco d'informazioni tra tutti i soggetti coinvolti, a voler garantire – particolarmente per le ipotesi che coinvolgono i *provider* di *VLOPs* e *VLOSEs* – non solo uno svolgimento ordinato delle attività, ma un assetto di *checks and balances* sull'esercizio dei penetranti poteri della Commissione.

Come osservato, emerge poi come proprio detti poteri siano descritti in termini decisamente più dettagliati di quanto non avvenga per quelli dei coordinatori – per i quali il regolamento rimette la scelta agli Stati membri, rinviando per la definizione delle condizioni e delle procedure specifiche al diritto nazionale. Si veda per raffronto, ad esempio, il grado di precisione della norma in tema di ispezioni della Commissione, che all'art. 69, par. 2, DSA, lett. da *a)* a *g)* puntualizza come queste possano consistere nell'accesso a tutti i locali, terreni e mezzi di trasporto del fornitore o dell'altra persona

[63] Con riferimento alle constatazioni preliminari della Commissione v. anche *infra*, par. 6.1.

[64] *Supra*, par. 3.

interessata; nell'esame dei libri e qualsiasi altro documento relativo alla fornitura del servizio in questione e nell'ottenimento di copie o estratti; nella richiesta di fornire accesso e chiarimenti relativi all'organizzazione, al funzionamento, al sistema informatico, agli algoritmi, alla gestione dei dati e alle pratiche commerciali dell'impresa nonché di registrare o documentare i chiarimenti forniti; nel sigillare i locali; nel chiedere chiarimenti e rivolgere domande a qualsiasi rappresentante o membro del personale in relazione a fatti o documenti inerenti all'oggetto e allo scopo dell'accertamento.
In coerenza con la previsione dell'art. 83 DSA che attribuisce alla Commissione il potere di adottare atti di esecuzione riguardanti le modalità pratiche per la conduzione di taluni procedimenti – tra cui ispezioni, audizioni e divulgazione negoziata di informazioni di cui all'art. 79 DSA – è stato adottato il relativo *implementing regulation*[65].
Nell'ambito di un procedimento che può portare all'adozione di una decisione di non conformità, la Commissione può con decisione ordinare misure provvisorie nei confronti del fornitore della piattaforma online o del motore di ricerca online di dimensioni molto grandi (art. 70 DSA), in caso di urgenza dovuta al rischio di danni gravi per i destinatari del servizio e sulla base di una constatazione *prima facie* della sussistenza di una violazione[66].
Da ultimo, è disposto che, qualora siano stati esauriti tutti i poteri della Commissione e la violazione persista, causando un danno grave non evitabile attraverso il ricorso a altri poteri previsti in ambito nazionale o dell'Unione, la Commissione europea possa sollecitare, a norma dell'art. 82 DSA, il coordinatore del luogo di stabilimento del fornitore della piattaforma online o del motore di ricerca online di dimensioni molto grandi interessato ad adire l'autorità giudiziaria per richiedere una restrizione all'accesso *ex* art. 51, par. 3, DSA.

6.1. *(Segue).* Le soluzioni "negoziate" per la definizione del procedimento tra Commissione e *very large online platform* e le sanzioni all'esito di *«non-compliance decisions»*

Se, nel corso di un procedimento avviato dalla Commissione, un *provider* della piattaforma online o del motore di ricerca online di dimensioni molto grandi si offre di assumere *impegni* (*commitment*) volti a garantire la conformità alle pertinenti disposizioni del DSA, si prevede che la Commissione possa, mediante decisione, rendere tali impegni vincolanti per quel fornitore, dichiarando che non vi sono ulteriori motivi per intervenire (art. 71, par. 1, DSA)[67].

[65] Regolamento di esecuzione (UE) 2023/1201 della Commissione del 21 giugno 2023 relativo alle modalità dettagliate di attuazione da parte della Commissione di determinate procedure a norma del regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio («regolamento sui servizi digitali»).

[66] L'art. 70, par. 2, DSA precisa che le tali decisioni si applicano per un periodo determinato e possono essere rinnovate «se necessario e opportuno».

[67] Rileva una qualche similitudine tra la logica di tali «soluzioni negoziate» volte a definire il procedimento e quella dei *non prosecution agreement* nordamericani E. Birritteri, *Punire la disinformazione*, cit., 315.

Ciò non mette, tuttavia, il fornitore in ogni caso al riparo dall'instaurazione di futuri procedimenti da parte della Commissione, che invero può – su richiesta o di propria iniziativa – riaprire il caso laddove, alternativamente: si verifichi un cambiamento determinante di uno dei fatti su cui si è fondata la decisione (lett. *a*); il fornitore in questione agisca in contrasto con i propri impegni (lett. *b*); la decisione sia stata fondata su informazioni incomplete, inesatte o fuorvianti trasmesse dal fornitore o da un'altra persona ai sensi dell'art. 67, par. 1, DSA.

D'altronde, la Commissione non è neppure tenuta ad accettare, per così dire, "a monte" tali impegni, ben potendo – ove ritenga che questi non siano idonei a garantire l'effettivo rispetto delle pertinenti disposizioni del regolamento – respingerli con decisione motivata al momento della conclusione del procedimento (art. 71, par., 3 DSA).

Lo svolgimento dei compiti della Commissione risulterebbe alquanto difficile da assicurare ove a essa non fosse consentito di intraprendere «le azioni necessarie per monitorare l'effettiva attuazione e osservanza» del DSA da parte di *VLOPs* e *VLOSEs* (art. 72 DSA). A tal fine, la Commissione può ordinare a tali soggetti di fornire accesso alle banche dati e agli algoritmi nonché spiegazioni al riguardo, oltre a poter imporre loro l'obbligo di conservazione di tutti i documenti ritenuti necessari. Nell'ambito del monitoraggio, la Commissione può anche avvalersi della consulenza di esperti e revisori esterni indipendenti o delle autorità nazionali competenti.

La Commissione può invece determinarsi all'adozione di una decisione di non conformità (*non-compliance decision*) nei casi di mancato rispetto, da parte del fornitore della piattaforma online o del motore di ricerca online di dimensioni molto grandi, di uno o più dei seguenti requisiti: le pertinenti disposizioni del DSA (lett. *a*); le misure provvisorie ordinate *ex* art. 70 DSA (lett. *b*); gli impegni resi vincolanti secondo le prescrizioni dell'art. 71 DSA (lett. *c*) (art. 73, par. 1, DSA)[68].

Considerate le conseguenze di una simile decisione, la relativa adozione è corredata da talune garanzie procedurali: la Commissione deve infatti comunicare le proprie constatazioni preliminari al soggetto interessato prima di procedere, illustrando le misure che intende prendere o che ritiene il fornitore in questione dovrebbe prendere in risposta alle constatazioni preliminari.

La decisione di non conformità contiene l'ordine al fornitore di adottare le misure necessarie a garantire il rispetto della medesima, specificando altresì un termine ragionevole per provvedere e richiedendo informazioni sulle misure che il destinatario preveda di adottare per rendersi *compliant*.

Con la decisione di non conformità *ex* art. 73 la Commissione può imporre al *provider* di *VLOPs* e *VLOSEs* sanzioni pecuniarie analoghe a quelle già esaminate con riferimento ai coordinatori dei servizi digitali nazionali, sebbene le casistiche non siano coincidenti. In particolare, la Commissione può imporre a tali soggetti sanzioni pecuniarie non superiori al 6 % del fatturato totale realizzato a livello mondiale su base annua nell'esercizio precedente (art. 74, par. 1, DSA) laddove essi, intenzionalmente o per negligenza, violino le pertinenti disposizioni del regolamento (lett. *a*), non rispettino una decisione

[68] L'esito procedimentale può anche condurre a ritenere le condizioni di cui all'art. 73, par. 1, DSA non soddisfatte, e in tal caso il par. 5 della medesima disposizione precisa che la Commissione dovrà chiudere l'indagine per mezzo di una decisione che si applica con effetto immediato.

che dispone le misure provvisorie di cui all'art. 70 DSA (lett. *b*) o non si conformino a un impegno reso vincolante ai sensi dell'art. 71 DSA (lett. *c*).
La sanzione in oggetto a carico di *VLOPs* e *VLOSEs* sarà invece non superiore all'1 % del reddito annuo o del fatturato totale annuo a livello mondiale dell'esercizio precedente – e potrà attingere anche un'altra persona fisica o giuridica ai sensi dell'art. 67, par. 1, DSA – se, in modo intenzionale o per negligenza, si verifichi uno dei seguenti casi: informazioni inesatte, incomplete o fuorvianti in risposta a una richiesta semplice o formulata mediante decisione; mancata risposta entro il termine stabilito alla richiesta di informazioni formulata mediante decisione; omessa rettifica entro i termini di informazioni inesatte, incomplete o fuorvianti, o omissione o rifiuto di fornire informazioni complete; rifiuto di sottoporsi a un'ispezione; mancato rispetto dei provvedimenti adottati dalla Commissione a norma dell'art. 72 DSA; mancato rispetto delle condizioni di accesso al fascicolo della Commissione *ex* art. 79, par. 4, DSA (art. 74, par. 2, DSA). Anche l'adozione di una decisione a norma del par. 2 appena descritto deve essere preceduta dalla comunicazione ai soggetti interessati[69] da parte della Commissione delle proprie constatazioni preliminari.
Quanto ai criteri di determinazione dell'importo della sanzione pecuniaria, deve tenersi conto della natura, della gravità, della durata e della reiterazione della violazione e, per le menzionate sanzioni di cui al par. 2 dell'art. 74 DSA, del ritardo causato al procedimento.
In linea generale, rispetto all'impianto complessivo, non può però farsi a meno di osservare come la proporzionalità della comminatoria astratta risulti alquanto sacrificata, avendo il legislatore accomunato sotto un unico "macro *range*" edittale fatti dal disvalore anche assai diverso[70] – *sub* art. 74, par. 1, lett. *a)*, sostanzialmente, qualsiasi violazione del regolamento – che, forse, più opportunamente si sarebbe potuto differenziare mediante cornici sanzionatorie autonome; ciò avrebbe contribuito, altresì, a rendere maggiormente prevedibile l'esito concreto dell'esercizio della potestà sanzionatoria da parte della Commissione.
Va poi segnalata la peculiare procedura di vigilanza rafforzata (*enhanced supervision*) da parte della Commissione sull'*enforcement* degli obblighi di cui al Capo III, sezione 5 (art. 75 DSA).
Nell'adottare una decisione di *non-compliance* che attenga, nella specie, alla violazione, da parte di una *VLOP* o di un *VLOSE*, di uno dei suddetti obblighi, la Commissione chiede al soggetto in questione «di elaborare e comunicare, entro un termine ragionevole specificato nella decisione, ai coordinatori dei servizi digitali, alla Commissione e al comitato un piano d'azione che stabilisca le misure necessarie, sufficienti per porre fine alla violazione o porvi rimedio». La norma chiarisce che le misure possono consistere nell'impegno a effettuare una revisione indipendente secondo quanto previsto dall'art. 37 DSA – dovendosi specificare l'identità dei revisori, la metodologia, la tempistica e il seguito da dare alla revisione – e a partecipare a un codice di condotta

[69] Oltre al fornitore della piattaforma online o del motore di ricerca online di dimensioni molto grandi si menziona anche «un'altra persona» *ex* art. 67, par. 1, DSA (art. 74, par. 3, DSA).

[70] V. già, per considerazioni di simile tenore nel contesto del GDPR, L. D'Agostino, *La tutela penale dei dati personali nel riformato quadro normativo*, cit., 21.

pertinente, ai sensi dell'art. 45 DSA.

L'*action plan* viene sottoposto dapprima al vaglio del Comitato, che entro un mese dal ricevimento deve trasmettere il proprio parere alla Commissione, la quale successivamente, entro un termine analogo, decide se le misure stabilite nel piano siano sufficienti – in ciò tenendo in conto l'eventuale impegno della *large platform* ad aderire ai codici di condotta pertinenti – fissando un termine ragionevole per la relativa attuazione. La Commissione deve, a seguire, monitorare l'implementazione del piano, e a questi fini il fornitore coinvolto deve trasmettere prontamente la relazione di revisione e aggiornamenti in merito alle misure adottate, potendo la Commissione richiedere informazioni supplementari.

Anche nel contesto della vigilanza rafforzata, la Commissione – laddove non riceva il piano d'azione (o gli altri documenti o informazioni sopra indicati) o ritenga di respingerlo, o lo consideri insufficiente a porre fine o a rimediare alla violazione – può infliggere penalità di mora (art. 76 DSA) e, nei casi previsti, come detto, può rivolgersi al coordinatore dei sevizi digitali del luogo di stabilimento e sollecitare una richiesta di restrizione all'accesso (art. 82, par. 1, DSA).

Più in generale, le penalità di mora ricalcano quelle a disposizione delle autorità nazionali e presidiano altresì gli obblighi di *VLOPs* o *VLOSEs* di fornire informazioni corrette e complete in risposta a una decisione, di sottoporsi a un'ispezione, di conformarsi a una decisione che dispone misure provvisorie, di rispettare gli impegni resi giuridicamente vincolanti da una decisione (art. 76, par. 1, DSA).

I poteri conferiti alla Commissione per l'irrogazione di sanzioni pecuniarie o penalità di mora (*ex* artt. 74 e 76 DSA) sono soggetti a un termine di prescrizione di cinque anni, decorrente dal giorno in cui è stata commessa la violazione (art. 77, par. 1 e par. 2, DSA)[71].

Il regolamento si premura di prevedere anche una disciplina degli atti interruttivi – elencati in via esemplificativa al par. 3 della disposizione[72] e coincidenti con «[q]ualsiasi azione intrapresa dalla Commissione o dal coordinatore dei servizi digitali ai fini dell'indagine o del procedimento in relazione a una violazione» – nonché casi di sospensione del termine di prescrizione – fin tanto che la decisione della Commissione sia oggetto di un procedimento dinanzi alla Corte di giustizia dell'Unione europea. Sebbene ogni interruzione comporti un nuovo decorso dal principio del termine di prescrizione, è stabilito altresì un termine prescrizionale massimo[73].

Anche il potere della Commissione di procedere all'esecuzione delle sanzioni si prescrive in cinque anni dal giorno in cui la decisione diventa definitiva, prevedendosi pure in questo caso regole in tema di atti interruttivi (art. 78 DSA)[74].

---

[71] Tuttavia, in caso di violazioni continuate o reiterate, tale termine decorre dal giorno in cui cessa la violazione (così ancora l'art. 77, par. 2, DSA).

[72] Rientrano nel novero degli atti interruttivi, in particolare, le richieste di informazioni da parte della Commissione o di un coordinatore dei servizi digitali, le ispezioni e l'avvio di un procedimento da parte della Commissione a norma dell'art. 66, par. 1, DSA.

[73] *Id est*, il decorso di un tempo pari al doppio del termine di prescrizione senza che la Commissione abbia irrogato una sanzione pecuniaria o una penalità di mora, eventualmente prolungato della durata della menzionata sospensione: cfr. art. 77, par. 4 e par. 5, DSA.

[74] L'art. 78, par. 3, DSA stabilisce che il termine di prescrizione per l'esecuzione delle sanzioni è

7. Rilievi conclusivi

Al termine della disamina condotta sull'assetto di *enforcement* pubblico del DSA è possibile tracciare un primo, essenziale bilancio della disciplina introdotta dal nuovo regolamento in questo campo.

Si è messo in evidenza come la cifra degli equilibri istituzionali risieda nel sistema "reticolare" che prevede una strutturata cooperazione tra le autorità coinvolte e tra l'ambito nazionale e quello europeo; in dottrina, non si è mancato di porre l'accento su questa caratteristica quale elemento distintivo rispetto ad altri, recenti modelli di regolazione della «trasformazione digitale», a cominciare dal regolamento "gemello" *Digital Markets Act* – come noto, parte dello stesso pacchetto[75] con cui è stato introdotto il DSA e in cui si rinviene un più marcato accentramento di poteri in capo alla Commissione – e dall'*AI Act* in corso di approvazione – in cui parrebbe prevalere la dimensione del decentramento[76].

Questa dinamica di collaborazione e la scelta di fare assegnamento sul ruolo di vari attori si espone, secondo talune letture, a possibili criticità sia dalla prospettiva delle autorità nazionali, sia da quella della Commissione europea.

Con riguardo ai coordinatori dei servizi digitali, si è già anticipato come una delle questioni chiave dell'intera attività di implementazione del DSA dipenderà da come gli Stati membri interpreteranno la designazione di tali soggetti. Anzitutto sul piano domestico, inevitabilmente si richiederà la cooperazione tra il coordinatore e le altre autorità nazionali che potrebbero avere voce in capitolo su questioni specifiche, come in materia di protezione dei dati, concorrenza, telecomunicazioni etc.[77]

In ottica multilivello, poi, nelle dinamiche di pesi e contrappesi che, come visto, sostengono i "rapporti di forza" tra Stati membri e Commissione, «i limiti intrinseci» alla strategia di individuazione dell'autorità nazionale competente basata sul luogo di stabilimento delle piattaforme – sulla scia dei problemi sperimentati con il GDPR, dato che la gran parte di queste ultime ha sede in pochissimi Stati membri – potranno comportare molteplici rischi: dalla erosione delle prerogative degli altri coordinatori statali, al «sovraccarico» per le amministrazioni nazionali interessate che potrebbero non essere in grado di svolgere in modo rapido ed efficace l'attività di vigilanza, sino al consequenziale esito di un rafforzamento del ruolo di "supplenza" della Commissione

interrotto: «a) dalla notifica di una decisione che modifica l'importo iniziale della sanzione pecuniaria o della penalità di mora, oppure respinge una domanda intesa ad ottenere una tale modifica; b) da qualsiasi azione della Commissione, o di uno Stato membro che agisca su richiesta della Commissione, volta a dare esecuzione al pagamento della sanzione pecuniaria o della penalità di mora». Ogni interruzione fa decorrere nuovamente il termine di prescrizione dal principio.

[75] In argomento v. M. Eifert - A. Metzger - H. Schweitzer - G. Wagner, *Taming the giants: The DMA/DSA package*, in *Common Market Law Review*, 2021, 987 ss. Per una chiave di lettura focalizzata sull'impatto socio-economico dei due regolamenti in discorso, v. il recente studio di F. Decarolis - M. Li, *Regulating Online Search in the EU: From the Android Case to the Digital Markets Act and Digital Services Act*, in *International Journal of Industrial Organization*, 90, 2023, 1 ss.

[76] Questa la lettura di L. Torchia, *I poteri di vigilanza*, cit., 1106 ss. e 1110 ss. Sulle potenziali interferenze applicative, in particolare, tra DSA e *AI Act*, v. S. Tommasi, Digital Services Act *e* Artificial Intelligence Act: *tentativi di futuro da armonizzare*, in *Persona e mercato*, 2, 2023, 279 ss.

[77] F. G'sell, *The Digital Services Act*, cit., 106.

europea nei casi di stasi[78].

Inoltre, la normativa sottolinea, tra i requisiti delle autorità nazionali, quello dell'indipendenza: la circostanza che siano previsti casi di competenza concorrente ed esclusiva della Commissione solleva, secondo alcuni – trattandosi di una istituzione che ha il monopolio dell'iniziativa legislativa –, esattamente la questione della sua capacità di non subire, quale *enforcer* del DSA, condizionamenti legati alla propria agenda e ai propri obiettivi politici in ambiti correlati al regolamento[79].

Sul piano dei risvolti dei poteri di cui alla normativa, l'insieme delle previsioni prese in esame restituisce l'immagine di un sistema finalizzato in via principale alla tutela dell'utente che – contemperando l'afflittività di alcune delle misure introdotte con la costruzione di un apparato di garanzie[80] – replica nel contesto dei servizi digitali l'approccio *risk based* adottato in altri settori: merita attenzione l'imposizione, specialmente in capo alle grandi *corporation*, di puntuali obblighi di *compliance* autonomamente sanzionati, sulla falsariga di quanto già accaduto, nel contesto regolatorio europeo, ancora una volta in tema di *privacy* – o, ad attestare che si tratta di un *trend* trasversale in diversi ambiti – in materia di cybersicurezza[81] e di sostenibilità[82]. Se tale scelta appare condivisibile in vista di una massimizzazione del grado di effettività del DSA, come già rilevato permangono, tuttavia, talune perplessità sulle relative modalità di attuazione: si pensi alla previsione, sostanzialmente, di una unica macro cornice edittale nell'ambito delle sanzioni pecuniarie applicabili da parte della Commissione, per violazioni di – anche notevole – diverso disvalore[83].

Concludendo, in definitiva resterà da vedere come gli attori pubblici – Stati membri e Commissione – si orienteranno nel dare esecuzione alle disposizioni del nuovo regolamento.

Certamente sarà particolarmente importante provvedere, tramite ogni opportuna modifica normativa o regolamentare di raccordo, a implementare procedure efficaci per adempiere agli obblighi di cooperazione reciproci tra i soggetti coinvolti e per il migliore esercizio dei poteri di *enforcement* attribuiti dal DSA. A livello nazionale, ove emergeranno *gap* di disciplina sul punto, ciò comporterà la necessità di introdurre, in particolare, sanzioni amministrative per le violazioni del regolamento, conformemente

---

[78] V. in questo senso le riflessioni di G. Buttarelli, *La regolazione delle piattaforme digitali*, cit., 123.

[79] I. Buri, *A Regulator Caught Between Conflicting Policy Objectives*, cit., specie 79 s.

[80] Di una «'riedizione' dell'effetto di Bruxelles di cui si è detto a proposito dell'esportazione del *GDPR*, ma questa volta fondato più su un *humus* procedurale che assiologico-sostanziale, e quindi meno suscettibile di crisi di rigetto» parla O. Pollicino, voce *Potere digitale*, in *Enciclopedia del diritto*, *I tematici*, V, Milano, 2023, 442.

[81] Il riferimento è, ad esempio, agli obblighi di adozione di misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi per la sicurezza delle reti e dei sistemi informativi e di notifica degli incidenti da parte degli operatori di servizi essenziali e fornitori di servizi digitali di cui alla direttiva (UE) 2016/1148 (NIS), il cui impianto è sostanzialmente confermato – pur con alcune novità, ad esempio sul piano dei destinatari della normativa – dalla recente direttiva (UE) 2022/2555 (NIS 2).

[82] Si veda la strada imboccata, in particolare, con la proposta di direttiva del Parlamento europeo e del Consiglio relativa al dovere di diligenza delle imprese ai fini della sostenibilità e che modifica la direttiva (UE) 2019/1937. Sul tema degli obblighi di *compliance*, v. da ultimo A. Gullo, *Compliance*, in *Archivio penale web*, 2, 2022, 8 ss.

[83] V. *supr*a, par. 6.1.

ai criteri ivi sanciti: ossia, dovrà trattarsi di «*penalties*» effettive, proporzionate e dissuasive e in linea con i limiti massimi edittali previsti. Dovrà, del pari, essere oggetto di regolamentazione il correlato procedimento di applicazione delle sanzioni, nel rispetto dei principi di garanzia richiamati dal DSA (tra l'altro, tutela del diritto di difesa, diritto di essere ascoltati e di accedere al fascicolo, diritto a un ricorso giurisdizionale effettivo, secondo quanto stabilito dall'art. 51, par. 6 del regolamento)[84].

[84] Cfr. sul punto la scelta operata, come si è detto, dal legislatore italiano, che ha demandato all'AGCOM, in qualità di coordinatore dei servizi digitali, di individuare le modalità di applicazione delle sanzioni secondo procedure stabilite con proprio regolamento.

Aggiornamento delle indicazioni di *policy*

In linea con i precedenti due cicli della ricerca, sono qui pubblicate le indicazioni di *policy* finali che raccolgono i vari spunti e le diverse indicazioni delle sezioni della ricerca. Occorre evidenziare, come necessaria premessa metodologica, che in considerazione del significativo mutamento del quadro normativo e istituzionale di riferimento, segnato dalla definitiva approvazione del DSA, diverse indicazioni di *policy* – specie quelle rivolte, nei precedenti cicli di indagine, ai decisori pubblici – sono state eliminate o riformulate *ex novo* in quanto non più in linea con il rinnovato panorama regolamentare (per cui, ad es., è ormai da escludersi che i singoli Stati membri possano intervenire in materie dettagliatamente disciplinate dal regolamento europeo). In conformità agli scopi e all'ambito tematico di riferimento di questa ricerca, e in continuità con i primi due cicli dello studio, va infine chiarito che tali indicazioni di *policy* sono state formulate avuto specifico riguardo al contrasto alle operazioni di disinformazione, considerando, pertanto, i principali adempimenti in tal senso pertinenti imposti dal *Digital Services Act* e dalle altre norme applicabili.

Indicazioni di *policy* per piattaforme e motori di ricerca online

n°	Descrizione
IP-01	**Nomina di *compliance officer* (ove applicabile ex art. 41 DSA)** – Nominare uno o più responsabili di *compliance* per la gestione dei rischi legati alla disinformazione, attribuendo tra l'altro a tale funzione il potere di sovraintendere a tutti gli adempimenti connessi alla DSA *compliance*, nonché poteri di impulso e verifica con particolare riguardo alle correlate azioni di *risk-assessment* e *risk-management*. È opportuno valutare l'istituzione di tale figura anche nelle organizzazioni che non rientrano nel raggio applicativo dell'art. 41 DSA e in conformità ai criteri ivi rinvenibili.

IP-02	**Procedure di valutazione dei rischi (ove applicabile *ex* art. 34 DSA)** – Predisporre idonee procedure di valutazione dei rischi legati alla diffusione di informazioni false, analizzando su base almeno annuale gli ambiti tematici (es. categorie, *hashtag*, profili) più esposti e prevedendo in relazione ad essi adeguate misure di contenimento del rischio in base al livello di rischio misurato. Le procedure dovranno considerare in particolare i rischi legati alla diffusione di notizie false atte a turbare l'ordine pubblico, la sicurezza e la salute pubblica, il dibattito democratico su temi di preminente interesse pubblico. Le piattaforme online e i motori di ricerca di grandi dimensioni dovranno altresì valutare eventuali rischi sistemici derivanti dall'erogazione dei propri servizi e assicurare il rispetto dei principi sanciti dall'art. 34 del DSA. È opportuno che anche le organizzazioni non soggette all'applicazione obbligatoria di quest'ultima previsione svolgano simili attività e applichino anche su base volontaria, pur tenendo conto delle proprie specificità operative, i principi sanciti da tale previsione del regolamento.
IP-03	**Attuazione e monitoraggio di misure di attenuazione dei rischi** – Predisporre idonee misure per attenuare i rischi identificati ai sensi della procedura di valutazione di cui all'IP-02 e costruire e implementare procedure per verificare l'effettiva attuazione delle misure di contenimento dei rischi in parola, assicurandone il miglioramento continuo. Le piattaforme dovrebbero coordinare le *policies* di contrasto alla disinformazione con i sistemi di gestione interni e con le procedure di controllo della qualità dei servizi resi e della sicurezza delle informazioni. Le piattaforme online e i motori di ricerca di grandi dimensioni dovranno conformarsi agli obblighi sanciti dall'art. 35 del DSA. È opportuno che anche le organizzazioni non soggette all'applicazione obbligatoria di quest'ultima previsione svolgano simili attività e applichino anche su base volontaria, pur tenendo conto delle proprie specificità operative, i principi sanciti da tale previsione del regolamento.
IP-04	**Audit interni e revisioni esterne indipendenti (ove applicabile *ex* art. 37 DSA)** – Prevedere su base almeno annuale lo svolgimento di audit interni, sotto la supervisione dei responsabili indicati nella IP-01, volti a valutare la conformità delle procedure interne con le fonti di *soft law* (codici etici e di condotta, linee guida, indicazioni di *policies* etc.) e con le norme cogenti di legge con particolare riguardo al DSA. Le piattaforme online e i motori di ricerca di grandi dimensioni dovranno conformarsi agli obblighi sanciti dall'art. 37 del DSA, richiedendo una revisione indipendente esterna. È opportuno, ad ogni modo, che anche le organizzazioni non soggette all'applicazione obbligatoria di quest'ultima disposizione valutino l'opportunità di sottoporsi periodicamente a *audit* esterni indipendenti.

IP-05	**Informativa agli utenti** – Includere nelle condizioni generali del servizio idonee previsioni contrattuali volte a vietare la diffusione di notizie false ove ciò costituisca reato o contenuto illegale ai sensi dell'art. 3, lett. h), del DSA. Predisporre, sui propri applicativi, idonee interfacce affinché l'utente possa agevolmente reperire tali previsioni contrattuali.
IP-06	**Sistemi di segnalazione delle informazioni illecite o lesive delle condizioni d'uso del servizio. Provvedimenti conseguenti sui contenuti e denunce all'Autorità. Strumenti e procedure di cooperazione con le Autorità anche in caso di crisi** – Predisporre strumenti e interfacce per consentire agli utenti di segnalare la presenza nel servizio di informazioni illecite o lesive delle condizioni d'uso del servizio. Predisporre procedure interne di esame tempestivo della segnalazione, che assicurino l'immeditata attuazione dei correlati provvedimenti ai sensi del DSA. Prevedere che venga altresì data notizia all'autore del contenuto dei provvedimenti adottati e degli strumenti di reclamo disponibili. Le procedure di segnalazione e l'obbligo di fornire motivazioni sui connessi provvedimenti devono essere svolte dalle piattaforme in conformità a tutti gli obblighi di dettaglio definiti in particolare dagli artt. 16 e 17 del DSA. Predisporre procedure interne, tempestive ed efficaci, per rimuovere contenuti illegali ai sensi dell'art. 9 del DSA, in relazione alla ricezione di ordini delle autorità pubbliche, e per notificare sospetti reati nei limiti di quanto specificamente previsto dall'art. 18 del DSA. Prevedere procedure dettagliate ed efficaci per assicurare una pronta esecuzione degli obblighi connessi all'eventuale attivazione da parte della Commissione europea di un meccanismo di risposta alla crisi *ex* art. 36 del DSA. Valutare altresì la partecipazione ai correlati protocolli di crisi *ex* art. 48 DSA. Assicurare l'accesso ai propri dati ai sensi dell'art. 40 DSA.

IP-07	**Definizione delle condizioni d'uso del servizio, delle sanzioni disciplinari e dei reclami –** Definire le regole d'utilizzo del servizio nel rispetto dei fondamentali principi di garanzia sanciti dalle Carte europee dei diritti (su tutti, il diritto alla libertà di espressione dell'utente) e in conformità agli obblighi definiti in dettaglio dagli artt. 14 e 15 del DSA. Non prevedere un generale divieto di condivisione di notizie false, ma introdurre, con un approccio caso per caso, divieti ben circoscritti e tassativi di diffondere certi contenuti, nonché relativi – anche a prescindere dal contenuto dell'informazione – a specifiche modalità fraudolente di utilizzo del servizio (ad. es. interazione artificiosa tra più *account*), con riferimento a singoli settori sensibili identificati tramite le attività di cui alla IP-02. Disciplinare le violazioni e le collegate misure di carattere sanzionatorio/interdittivo – dalla etichettatura o rimozione del contenuto, al blocco temporaneo al servizio, fino alla sospensione temporanea o permanente dell'*account* – nel rispetto, oltre che dei principi sanciti dal DSA e in particolare dall'art. 14, delle correlate minimali garanzie *sostanziali* e *procedurali*, tra cui, ad es.: il principio di legalità delle violazioni e delle misure sanzionatorie/interdittive, con i relativi corollari della irretroattività, della tassatività/precisione delle previsioni punitive, e del divieto di analogia, con una chiara definizione dei soggetti titolari della potestà di dettare tali regole; il principio di proporzionalità del trattamento sanzionatorio rispetto alla concreta gravità della violazione; il divieto di responsabilità oggettiva e l'affermazione del principio di colpevolezza, con la necessità di specificare l'elemento soggettivo (dolo o colpa) necessario per integrare la violazione. Assicurare un elevato livello di trasparenza e dettaglio nel rendere pubbliche le modalità di funzionamento e le specifiche fasi delle procedure interne di applicazione delle misure sanzionatorie/inibitorie e per la gestione dei reclami da parte degli utenti, nel rispetto di minimali diritti procedurali, specie per ciò che concerne il diritto al contraddittorio preventivo e la garanzia di autonomia e indipendenza (con riferimento alla distribuzione dei poteri dell'organizzazione) dei soggetti deputati a irrogare la sanzione e a decidere sui connessi reclami; il diritto di richiedere il riesame della decisione già a livello interno, etc. Per le piattaforme online e i motori di ricerca occorre altresì conformarsi agli obblighi sanciti dagli artt. 20, 21 e 22 del DSA. È opportuno che anche gli operatori non soggetti all'applicazione di queste ultime previsioni predispongano sistemi interni di reclamo e meccanismi di cooperazione con segnatori attendibili in conformità alle previsioni in parola e ai principi generali di cui alla presente indicazione di *policy*.

IP-07-*bis*	**Misure specifiche a garanzia del pluralismo dell'informazione nella definizione delle condizioni d'uso del servizio** – Prevedere misure specifiche e puntuali, nella definizione delle condizioni d'uso del servizio, a tutela del pluralismo dell'informazione e della garanzia per tutti i media della possibilità di poter accedere e condividere i propri contenuti in piattaforma in condizioni di piena ed effettiva parità. Prevedere delle garanzie rafforzate per quanto attiene alle attività di moderazione dei contenuti immessi da tali operatori dell'informazione, nel rispetto della cornice generale delle misure a protezione dei diritti degli utenti definite ai sensi della IP-07.
IP- 08	**Pubblicità online** – Istituire un registro di informazioni chiare, corrette e trasparenti in merito all'identità o a caratteristiche di terzi che sponsorizzano propri prodotti o servizi sulla piattaforma. Imporre ai professionisti (es. agenzie di *marketing*, intermediari etc.) che si avvalgono dei servizi di pubblicità intra-piattaforma di indicare il nominativo del cliente e/o il titolare effettivo dell'annuncio che sarà mostrato sulla piattaforma. Prevedere procedure di controllo, anche a campione, sulle pubblicità mostrate dalla piattaforma in ambiti ritenuti a rischio ai sensi della IP-02. Annotare nel registro anche il periodo durante il quale è stata presentata la pubblicità e il novero di soggetti a cui era rivolto, nonché i parametri utilizzati per individuare i destinatari. Assicurare, nel predisporre tali procedure, il rispetto delle previsioni di cui all'art. 39 del DSA.
IP-09	**Verifiche sugli operatori business** – Prevedere procedure di controllo, anche a campione, sui contenuti diffusi da operatori *business* (es. profili *social* di grandi imprese, istituzioni, ONG, profili di persone politicamente esposte) attivi in ambiti ritenuti a rischio ai sensi della IP-02. Assicurare che le segnalazioni relative a tali operatori siano trattate in via prioritaria rispetto alle altre segnalazioni. Sottoporre a tali operatori una informativa sulle procedure, le misure e gli strumenti applicabili alle condotte di disinformazione sulla piattaforma, in modo da ottenere una presa d'atto per accettazione. Prevedere procedure di tracciabilità degli operatori *business*. Qualora tali operatori intendano pubblicizzare o offrire prodotti o servizi, la piattaforma dovrà previamente acquisire (*ex* art. 30 DSA, ove applicabile) i dati identificativi dell'impresa (es. denominazione, estremi dell'iscrizione nel registro delle imprese, dettagli relativi al conto di pagamento), oltre a un'autocertificazione relativa alla conformità dei prodotti o servizi offerti alle norme dell'Unione.

IP-10	**Codici di condotta** – Adottare strumenti di regolazione flessibile e *best practices* per il contenimento dei rischi legati alla disinformazione, aderendo se del caso a codici di condotta già esistenti elaborati da enti o istituzioni qualificate. Prevedere, con riferimento a tali strumenti, procedure e controlli particolari in contesti e periodi temporali particolarmente esposti al rischio di disinformazione (es, periodi precedenti alle elezioni politiche, contesti emergenziali). Verificare periodicamente l'avvenuta adozione *ex* art. 45 DSA di codici di condotta a cui la piattaforma possa aderire.
IP-11	**Algoritmi di raccomandazione –** Svolgere controlli periodici ed effettuare *algorithm auditing* sui parametri utilizzati dai sistemi di raccomandazione dei contenuti presenti sulla piattaforma, con particolare riguardo agli ambiti tematici a rischio di disinformazione ai sensi della IP-02. Prevedere misure atte a prevenire che un contenuto afferente a tali ambiti (specie contenente informazioni false costituenti contenuto illegale o la cui condivisione sia vietata dalle condizioni d'uso del servizio definite nel rispetto dei principi di cui alla IP-07) possa essere "consigliato" dagli algoritmi di raccomandazione, diventando così "virale" nel web, senza che detti algoritmi siano stati sottoposti a controllo o validazione, anche in osservanza degli standard internazionali applicabili. Specificare nelle condizioni generali *ex* art. 27 o 38 DSA (ove applicabili) i principali parametri utilizzati dagli algoritmi di raccomandazione, nonché qualunque opzione che consenta all'utente di modificare tali parametri. Assicurare almeno un'opzione non basata sulla profilazione.
IP-12	**Report periodici –** Pubblicare almeno una volta all'anno *ex* art. 15 DSA un report sulle attività di moderazione dei contenuti, che includa tutti i dettagli previsti da tale disposizione. Tale relazione dovrà essere altresì redatta in conformità all'art. 42 DSA per quanto riguarda piattaforme online e motori di ricerca di dimensioni molto grandi.
IP-12-*bis*	**Conservazione dei contenuti rimossi e della documentazione connessa a ogni misura di moderazione dei contenuti degli utenti che sia stata adottata –** Conservare, in appositi archivi online, i contenuti rimossi e la documentazione connessa a ogni misura adottata all'esito dell'attività di moderazione dei contenuti degli utenti svolta ai sensi e nel rispetto delle indicazioni della IP-07 e della IP-07-*bis* e prevedere la conservazione dei documenti relativi all'istruttoria svolta in modo da garantire la possibilità di ricostruire con chiarezza il percorso decisionale sfociato nella decisione di rimuovere il contenuto illecito o lesivo delle condizioni d'uso del servizio o di adottare qualsiasi altra misura in relazione allo stesso.

Indicazioni di *policy* per operatori e imprese non destinatari degli obblighi definiti dal DSA

n°	Descrizione
IP- 13	**Valutazione dei rischi** – Effettuare con cadenza almeno annuale la valutazione dei rischi legati alla diffusione di informazioni false sui canali *social* e sulle piattaforme utilizzate dall'impresa o dall'operatore. Analizzare in particolare gli ambiti di attività (es. linee di *business*, tipologie di prodotti etc.) particolarmente esposti al rischio di disinformazione e prevedere in relazione ad essi adeguate misure di contenimento del rischio in base alle risorse disponibili e al livello di rischio misurato. Le procedure dovranno considerare in particolare i rischi legati alla diffusione di notizie false atte a turbare l'ordine pubblico, la sicurezza pubblica, il dibattito democratico su temi di preminente interesse pubblico.
IP-14	**Gestione dei profili business** – Predisporre adeguate procedure organizzative e di controllo per l'utilizzo delle utenze e dei profili registrati su piattaforme online, prevedendo in particolare che i privilegi di amministratore della pagina e le credenziali di accesso siano attribuiti a soggetti all'uopo designati, sottoposti alla vigilanza di organi e funzioni di controllo.
IP-15	**Controllo sui contenuti** – Predisporre adeguate procedure di controllo da parte di responsabili aziendali prima della pubblicazione di notizie (es. post, messaggi, articoli) su piattaforme online. Prevedere la necessità di una autorizzazione preventiva per la pubblicazione di contenuti ritenuti particolarmente sensibili in base agli esiti della valutazione dei rischi.
IP- 16	**Meccanismi di segnalazione degli** user-generated contents – Prevedere procedure di controllo sui contenuti diffusi da utenti privati e collegati alla pagina social dell'impresa (o dell'organizzazione) mediante il sistema dei *tag*. Segnalare senza indebito ritardo al gestore della piattaforma notizie non veritiere relative ad ambiti ritenuti a rischio, al fine di consentire l'applicazione dei provvedimenti conseguenti. Tale segnalazione dovrebbe essere effettuata anche nel caso in cui il contenuto diffuso dagli utenti non sia direttamente collegato alla pagina social dell'impresa (o dell'organizzazione), ma quest'ultima ne abbia comunque avuto conoscenza.

IP-17	**Doveri di diligenza per i professionisti dell'informazione** – Predisporre adeguate procedure di controllo sulla veridicità delle fonti e sul rispetto dei criteri di verità, pertinenza e continenza nell'attività giornalistica e di informazione su aree tematiche ritenute a rischio. Laddove il professionista dell'informazione (es. agenzie di stampa, operatori radio e televisivi, testate telematiche registrate, quotidiani *online*) disponga di una pagina su una piattaforma online, coordinare tali procedure di controllo con quelle previste dalla IP-15. Predisporre adeguate procedure di controllo sul rispetto delle disposizioni contenute in codici etici e di condotta al quale il professionista dell'informazione abbia aderito.
IP-18	**Codici di condotta** – Adottare strumenti di regolazione flessibile e *best practices* per il contenimento dei rischi legati alla disinformazione, aderendo ove possibile a codici di condotta già esistenti elaborati da enti o istituzioni qualificate. Tale misura dovrebbe essere seguita in particolare dalle organizzazioni che operano come professionisti dell'informazione.
IP-19	**Controlli sull'attività dei fornitori** – Prevedere procedure di controllo, anche a campione, sulle attività affidate in *outsourcing* a terzi fornitori (es. gestione del profilo social da parte di agenzie di stampa o di *marketing*) in ambiti ritenuti a rischio o ad essi connessi o correlati.

Indicazioni di *policy* per istituzioni pubbliche nazionali

n°	Descrizione
IP-20	**Costituzione di gruppi di lavoro e partnership con gli operatori privati** – In misura compatibile con gli obblighi del DSA, costituire – sotto la supervisione del coordinatore nazionale dei servizi digitali – tavoli di lavoro per la discussione sui temi della disinformazione e per incentivare il dibattito pubblico su questi temi. Diffondere la cultura della "buona informazione" nel rispetto del pluralismo democratico e della libertà di espressione, sensibilizzando i cittadini e gli operatori economici sui rischi legati alla manipolazione dell'informazione.

IP-21	**Analisi nazionale dei rischi legati alla disinformazione** – In conformità al DSA, e sotto la supervisione e l'impulso del coordinatore nazionale dei servizi digitali, intraprendere iniziative, anche attraverso il coordinamento tra pubbliche amministrazioni, per elaborare, su base almeno annuale, un documento riassuntivo dei rischi e delle priorità nazionali per ciò che concerne la lotta alla disinformazione. Il documento contenente l'analisi nazionale dei rischi dovrebbe essere pubblicato e reso facilmente accessibile per tutti gli operatori pubblici e privati.
IP-22	**Attuazione delle modifiche normative necessarie ad assicurare l'efficace applicazione del DSA** – Provvedere alla designazione del coordinatore nazionale dei servizi digitali in conformità al DSA, e assicurare, anche tramite ogni modifica normativa o regolamentare di necessario raccordo, l'implementazione di procedure efficaci per adempiere agli obblighi di cooperazione con la Commissione europea, e altre istituzioni, delineati dal nuovo regolamento europeo, nonché per assicurare il migliore esercizio dei poteri di *enforcement* nazionali ivi disciplinati. Sotto il profilo sanzionatorio, provvedere all'introduzione di sanzioni amministrative per la violazione del nuovo regolamento europeo in conformità ai criteri sanciti dagli artt. 51 e 52 del DSA, disciplinando altresì le regole connesse al correlato procedimento applicativo nel rispetto dei principi di garanzia stabiliti dall'art. 51, par. 6, del DSA (tra l'altro, tutela del diritto di difesa, diritto di essere ascoltati e di accedere al fascicolo, diritto a un ricorso giurisdizionale effettivo). Disciplinare sanzioni amministrative pecuniarie e penalità di mora, nonché eventuali connesse misure provvisorie ai sensi dell'art. 51 del DSA, che siano "effettive, proporzionate e dissuasive" nel senso richiesto dal già menzionato art. 52, par. 1, del DSA, e in linea con i limiti massimi edittali sanciti dai parr. 3 e 4 della stessa previsione.

Saggi

Digital Euro as a platform and its private law implications*

Vincenzo Zeno-Zencovich

Abstract

The article analyses, in the light of the various preparatory documents of a ECB digital currency and of two recent proposals of regulation by the EU Commission what are the private law implications of such an innovation, especially in the field of the law of obligations, and the consequences of the transformation of central banks in digital platforms.

Summary

Keywords

e-money – platforms – digital payments – data protection – monetary sovereignty

1. Introduction

The process of creating digital currencies with legal tender presents all the traditional problems of money, in addition to those common to the dematerialization of socio-economic relationships and activities.

Although we have been talking about "Central Bank Digital Currencies" (CBDCs) for less than twenty years[1], it should be noted that this outcome is only a further stage in

* Su determinazione della direzione, ai sensi dell'art. 15 del Regolamento, il contributo non è stato sottoposto a referaggio.

This paper was presented at the ELSOBA (European Legal Strategies for payment systems in the Open Banking Age) final conference at Siena university in October 2022. On June 28,2023 the EU Commission presented two twin proposals for a Regulation on the "legal tender of euro banknotes and coins" (henceforth the Legal tender Regulation) and on the "establishment of the digital euro" (henceforth the Digital euro Regulation). Inasmuch as possible this text takes into account the abovementioned proposals which in some cases confirm the analysis provided in the original paper, in other cases go in a different direction.

[1] P.K. Ozili, *Central bank digital currency research around the World: a review of literature,* in *Journal of Money*

a process which began centuries ago of dematerialization of currency with the transition from metal to paper[2] and then to scriptural money which has been associated, for almost a century, with the progressive and general abandonment of the principle of the convertibility in gold of the currency issued by a State[3].

These pages want to highlight some trajectories that characterize the process of creating CBDCs and in particular its private law aspects in the broad sense of the word, while being aware that these must be inserted in a highly regulated context, within which financial and geo-political policies and macroeconomics play a prominent role[4].

The points that will be addressed are:

a) CBDCs as legal tender.

b) The implications on the law of obligations.

c) Digital euro and the GDPR.

d) Regulatory limitations on the use of CBDCs.

e) The digital euro as a platform.

It should be noted that these reflections are limited to the process of creating the

Laundering Control, 2022. See also the rich section on the Bank for International Settlements; and G. Soderberg, *Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons*, 2022.

[2] It is worthwhile remembering – also in relation to the ongoing process in the PRC – what Marco Polo describes in his *Travels* (at the end of the 13th century): «The Emperor's Mint then is in this same City of Cambaluc (*now Peking*), and the way it is wrought is such that you might say he hath the Secret of Alchemy in perfection, and you would be right! For he makes his money after this fashion. (…) All these pieces of paper are [issued with as much solemnity and authority as if they were of pure gold or silver; and on every piece a variety of officials, whose duty it is, have to write their names, and to put their seals. And when all is prepared duly, the chief officer deputed by the Kaan smears the Seal entrusted to him with vermilion, and impresses it on the paper, so that the form of the Seal remains printed upon it in red; the Money is then authentic. Anyone forging it would be punished with death]. And the Kaan causes every year to be made such a vast quantity of this money, which costs him nothing, that it must equal in amount all the treasure in the world. With these pieces of paper, made as I have described, he causes all payments on his own account to be made; and he makes them to pass current universally over all his kingdoms and provinces and territories, and whithersoever his power and sovereignty extends. And nobody, however important he may think himself, dares to refuse them on pain of death». And the circumstance is confirmed a few years later by Ibn Battuta in his *Travels*: «Transactions are carried on with paper: they do not buy or sell either with the dirhem or the dinar; but should anyone get any of these into his possession, he would melt them down into pieces. As to the paper, every piece of it is in extent about the measure of the palm of the hand and is stamped with the King's stamp. Five and twenty of such notes are termed a 'shat'; which means the same thing as a dinar with us. But when these papers happen to be torn, or worn out by use, they are carried to their house, which is just like the mint with us, and new ones are given in place of them by the King. This is done without interest; the profit arising from their circulation accruing to the King. When anyone goes to the market with a dinar or a dirhem in his hand, no one will take it until it has been changed for these notes».

[3] S. Grünewald - C. Zellweger-Gutknecht - B. Geva, *Digital Euro and ECB Powers*, in *Common Market Law Review*, 2021, 1035 highlight «the evolution of the concept of the banknote, of which the transition from paper to digital merely constitutes the latest in a sequence of evolutionary steps». See also S. Grünewald - C. Zellweger-Gutknecht – B. Geva, *Digital euro, monetary objects and price stability—A legal analysis*, in *J. Financial Regulation,* 284, 2021; S. Grünewald - C. Zellweger-Gutknecht – B. Geva, *The e-banknote as a 'banknote': A monetary law interpreted*, in *Oxford J. Legal Studies*, 2021, 1119, and R. De Bonis - M.I. Vangelisti, *Moneta*, Bologna, 2019.

[4] C. Herrman - C. Dornhacher, *International and European Monetary Law. An Introduction*, Berlin, 2017, 14 who point out the erosion of "monetary sovereignty" «due to limitations caused by globalization, information technology and economic and financial developments in the past decades».

digital euro, promoted by the European Central Bank[5] and to the two ensuing proposals issued by the EU Commission which are mutually connected: A Regulation on the establishment of the digital euro; and a Regulation on the legal tender of euro banknotes and coins. Therefore, although there are numerous parallel initiatives underway in other countries – in particular in the People's Republic of China[6], in the United States of America[7] and in European countries not belonging to the EU and the Eurosystem[8] – in this paper the problems of a digital currency will be referred to the fairly homogeneous legal framework in continental Europe.

Furthermore, it is necessary to clarify that the very complex issues relating to the powers of the ECB to issue the digital euro will not be considered. Questions whose solution lies in the Lisbon Treaties, as they will be interpreted by the Council which, ultimately, will be left with the decision whether, and with what modalities, this currency can be issued[9]. A decision that cannot fail to have repercussions also on its private law dimension.

Finally, again by way of premise, it should be specified that this paper shall not consider the phenomena of issuance by private subjects of digital entities whose aim was that of replacing the State currencies (the so-called crypto-currencies), and which – to any critical observer – had immediately revealed their purely speculative nature, many of which have been subject to fraud and embezzlement.

2. Digital Euro as Legal Tender

An Italian lawyer, grown up under the light of art. 1277 of the Civil Code[10], links the currency issued by a central bank to the notion of legal tender with the double function of means of determining the value of something, and of means of payment. On the one hand, prices, counter-prestations, resources and relationships are expressed in a current currency; and on the other hand, any pecuniary obligation, whether of a private or of a public nature, must be fulfilled - subject to express exceptions - through

[5] Over the last years the ECB has issued several Reports starting with an initial scepticism and subsequently moving forward very rapidly. See e.g., the Report Progress on the investigation phase of a digital euro, 29.9.2022; and the Paper Central bank digital currency and bank intermediation, May 2022. The main policy lines have been made explicit in numerous speeches by the member of the ECB's governing board.

[6] E. Journey Fullerton - P.J. Morgan, *The People's Republic of China Digital Yuan: Its Environment, Design, and Implications*, in Asian Development Bank Institute Discussion Paper no. 1306, February 2022.

[7] Report of the Federal Reserve Money and Payments: The U.S. Dollar in the Age of Digital Transformation, January 2022.

[8] For the UK see the Bank of England publications Central Bank Digital Currency Opportunities, challenges and design, March 2020; M. Kumhof - C. Noone, *Central bank digital currencies — design principles and balance sheet implications*, in Bank of England Working Paper no. 725, May 2018; O. Ward - S. Rochemont, *Understanding Central Bank Digital Currencies (CBDC)*, March 2019. For Sweden see the Sveriges Riksbank Report E-krona pilot Phase 2, April 2022.

[9] A. Dorsé - X. Barrull, *Special-purpose Central Bank Digital Currencies: A proposal*, available at SSRN (May 16, 2022).

[10] «Pecuniary obligations are discharged through a payment in the currency which has legal tender in the State at the moment of the payment and at nominal amount».

a currency which is legal tender.

However, when one observes the various systems of the Eurozone[11], one realizes that, at least formally, this framework is not common, *i.e.* not all of the following three elements are always recognized:

a) The obligation to receive a payment in currency having legal tender in the legal system that governs the obligation, unless the parties have previously agreed on different methods.

b) The nominalistic principle, according to which the payment due corresponds to the face value indicated by the currency – in coins/banknotes – having legal tender.

c) The discharging nature of the exact payment in legal tender currency with the consequence of extinguishing the obligation[12].

Although it could be assumed that the lack of a common notion of legal tender purely theoretically could have practical effects[13], to the extent that in the Eurozone all three

[11] The issue of the *lex monetae* and how it should be determined is analysed by M. Perassi, *Il diritto comunitario dei pagamenti*, in G. Carriero - V. Santoro, *Il diritto del sistema dei pagamenti*, Milan, 2005, 141.

[12] The necessary consequence is that the Legal tender Regulation must harmonize the various European rules by stating (art. 4) that:

«1. The legal tender status of euro banknotes and coins shall entail their mandatory acceptance, at full face value, with the power to discharge from a payment obligation.

2. In accordance with the mandatory acceptance of cash, the payee shall not refuse euro banknotes and/or coins tendered in payment to comply with that obligation.

3. In accordance with the acceptance at full face value of cash, the monetary value of euro banknotes and/or coins tendered in settlement of a debt shall be equal to the amount in euro indicated on the banknotes and/or coins. Surcharges on the settlement of debt with euro banknotes and coins shall be prohibited.

4. In accordance with the power to discharge from a payment obligation, a payer shall be able to discharge from a payment obligation by tendering euro banknotes and coins to the payee».

And the Digital euro Regulation *par consequence* states (art. 7) that:

«1. The digital euro shall have legal tender status.

2. The legal tender status of the digital euro shall entail its mandatory acceptance, at full face value, with the power to discharge from a payment obligation.

3. In accordance with the mandatory acceptance of the digital euro, the payee shall not refuse digital euro tendered in payment to comply with that obligation.

4. In accordance with the acceptance at full face value of the digital euro, the monetary value of digital euro tendered in payment of a debt shall be equal to the value of the monetary debt. Surcharges on the payment of debt with the digital euro shall be prohibited.

5. In accordance with the power of the digital euro to discharge from a payment obligation, a payer shall be able to discharge himself from a payment obligation by tendering digital euro to the payee».

The provision follows the indications of the Report by the Euro Legal Tender Group, (ELTEG), 2009 on "definition, scope and effects of legal tender of euro banknotes and coins": «Looking for a common definition of legal tender of euro cash, the Group expressed unanimous support for a definition relying on three main criteria, seen as cumulative, in cases where a payment obligation exists: a) Mandatory acceptance of euro cash; a means of payment with legal tender status cannot be refused by the creditor of a payment obligation, unless the parties have agreed on other means of payment. b) Acceptance at full face value; the monetary value of a means of payment with legal tender status is equal to the amount indicated on the means of payment. c) Power to discharge from payment obligations; a debtor can discharge himself from a payment obligation by transferring a means of payment with legal tender status to the creditor». One should however remember what has been aptly pointed out by A. Di Majo, *Il diritto comunitario dei pagamenti pecuniari*, in *Annuario del contratto,* 2010: the discharging effects of payments in a currency having legal tender does not aim so much at protecting the parties of the transaction, but to reassert the sovereignty of the State over the money it issues.

[13] H. Siekmann, *Legal tender in the euro area*, in IMFS Working Paper Series, Frankfurt, 2018 «In the euro area the *jus monetae* has been completely transferred to the EU with the result that the concerned

of these elements are not always found, the question has a great significance with regard to the proposal of a digital euro.

In the first place, while metal coins or banknotes are characterized by materiality and their delivery constitutes a juridically decisive act, with a digital - and therefore immaterial - currency, in the first place an appropriate technological instrumentation is needed to give the order, to transmit it, to receive it, failing which the currency is useless.

Secondly, there is a common principle in digital systems, namely that what is not regulated is free. Therefore, if the digital euro is to have all three of the characteristics indicated, it is necessary that they are expressly - and not indirectly - provided for.

On the other hand, systems with a Roman law tradition collide, always in the digital ecosystem, with the dilemma of whether we are faced with proprietary legal forms, characterized by the materiality of the asset, or, instead, with credit relationships, characterized by immateriality[14]. The difference is clear when one thinks of the instruments of criminal protection: the unlawful appropriation of banknotes constitutes the crime of theft or those of embezzlement or robbery. The "misappropriation" or "diversion" of digital euros by someone who is not entitled entails entirely different - and special - provisions in which the material element of the crime is of a different nature.

In addition, it should be noted that with the digital euro a further process of abstraction takes place: When the gold standard ruled, banknotes represented a credit towards the central bank. Once the gold standard has been abolished, banknotes maintain the nature of bearer instrument with a limited claim against the issuer, such as the replacement of deteriorated banknotes or with newly issued ones or with a new currency (as one has seen in the transition from national currencies to the euro). With the digital euro, the "purchase" of digital euros obliges the issuing institution to make them available (first abstraction) in order to then be able to use them as payment instruments recognized by the same institution (second abstraction).

All this leads to the construction of a system in which digital money, rather than moving between reality (banknotes) and abstraction (credit), is born, lives and ends as a credit situation[15].

But who is the "debtor"? The issuing institution, or the individual credit institutions authorized by the central bank to issue the digital currency?[16]

To this dilemma we must add further problematic aspects.

Member States lost their power to define legal tender, Art. 3.1 (c) TFEU».

[14] «The fact that money, with the end of metallism, is an abstract 'ideal unit', completely dematerialised and unconvertible, entails that it is not a commodity but rather a 'function', which serves as a medium of exchange and as a measure of value». N. Vardi, *The Integration of European Financial Markets*, London-New York, 2011, 3.

[15] A. Di Majo, *Il diritto comunitario dei pagamenti pecuniari*, cit., pointed out in his commentary to directive 2004/64 that payments had lost any "real" (in a civilian sense) nature and that payments have become services, and therefore are the object of a prestation and not of a delivery (of banknotes or coins).

[16] S. Grünewald - C. Zellweger-Gutknecht - B. Geva, *Digital Euro and ECB Powers*, cit., ask themselves if the digital euro should be considered a banknote (and therefore within the exclusive competence of the ECB) or a coin (and therefore within the competence of the Eurozone central banks. The Digital euro Regulation opts for the first choice.

When the digital euro is in someone's e-wallet, a unique and certified relationship is created between that amount and the holder. That value - marked with an alpha-numeric sequence expressed in univocal binary impulses - is and can only be in the possession of a certain subject, who can - and only he can - decide its destination: to continue to remain in the wallet, to be transferred to that of another person, to flow into a bank account, to be converted into cash.
This situation highlights the not always clear boundary - in a civil law environment - between property rights and credits. The "tokenization" of the digital euro[17] increases the uncertainty of the borders in the event of an off-line payment, *i.e.* without the use of the network that connects the holder's e-wallet to the central register of the issuer (or one of its intermediaries) and the latter to the e-wallet of the recipient[18]. Digital currency would almost be reified with an unintermediated passage from the payer to the payee.
On the other hand, in the hypothesis in which the issuing institution authorizes a credit institution to issue a certain amount of digital euros, what is the difference between these and the consolidated figure of "scriptural money"? It should be noted that with regard to the latter, the events concerning the credit an individual or an entity have towards the credit institution are regulated by a private law contract which establishes terms and conditions for deposits, withdrawal, overdrafts etc. But with regards to the digital euro, this exists and can only exist through a *fiat* of the issuing institution to which events of digital forgery or embezzlement could be referred.
Further profiles of ambiguity emerge in the case of loss of the e-wallet, which will usually be incorporated into a mobile phone necessarily equipped with functions (password, biometric identification, etc.) that make it usable only by the owner. Should one apply the traditional procedures used for the cancellation of material securities which have gone lost or destroyed?

3. The Implications on the Law of Obligations

With the digital euro, what changes in the law of pecuniary obligations? The attempt to answer is here confined to Italian law. It is, in fact, an area - that of pecuniary obligations - which has historically evolved under the influence of strong doctrinal writings, of very luxuriant negotiating practices, of a jurisprudential harvest that has adapted to the infinite variety of cases of conflict. To all this one must add the not infrequent legislative interventions that have touched this or that aspect.
It would therefore be impossible - here - to identify a trajectory in the French[19] or

[17] «The discussion thus naturally centres around a digital euro in the form of immaterial tokens recorded on the liability side of central banks' balance sheets and circulating in the economy through the transfer of these tokens (*i.e.* a token-based digital euro)». S. Grünewald - C. Zellweger-Gutknecht - B. Geva, *Digital Euro and ECB Powers*, cit.

[18] The Digital euro Regulation expressly provides that «The digital euro shall be available for both online and offline digital euro payment transactions».

[19] T. Le Gueut, *Le paiement de l'obligation monétaire en droit privé*, Librairie générale de droit et de jurisprudence, 2016.

German[20] legal systems where the issue of pecuniary obligations has always been the subject of in-depth and enlightening academic treatises. Clearly if and when the twin Regulations on legal tender and digital euro will have been approved there will be a convergence, but for a long-time path-dependency will govern the field[21].

a) With reference to the three characteristics of the currency indicated above, the first and preliminary question concerns the obligation to receive a payment in legal tender currency[22].

As has been said, the functionality of the digital euro depends on the availability of a technological device to credit the currency, a transmission network, and a device to receive it.

If these elements do not exist, the operation becomes very problematic: it cannot be transmitted, or the beneficiary is not able to verify that it has actually been carried out. And the difficulties exist even when the payment is made offline because the two devices (of the payer and of the payee) must be connected. A situation similar to that of the millionaire lost in the desert who would be willing to pay anything for a glass of water, but his unlimited credit card is useless.

Therefore, for the digital euro - unlike the physical currency - it would not seem possible to impose the obligation to accept it as a payment solution[23].

And yet the conclusion opens to an infinite number of variables drawn from the widespread use of IT payment instruments.

i. The obligation to accept a digital payment - instead of physical cash – may be imposed by contractual terms and conditions, *e.g.* already in the case of online purchases of goods and services, but also in many physical outlets that do not have a cash service. Or it can be imposed through legislation, such as the numerous interventions aimed at "limiting the use of cash". Sometimes, both forms of payment are possible, sometimes, above a certain amount, only the electronic one is possible. The Digital euro Regulation proposes rather broad exceptions (at art. 9) for small enterprises and non-profit entities (provided they do not accept other forms of digital payment)

[20] P.W. Heermann, *Geld und Geldgeschäfte*, Hamburg, 2003.

[21] The ECJ has repeatedly stated (see *ex multis* cases ECJ, C-489/15, *CTL Logistics* (2017) and ECJ, C-484/20, *Vodafone Kabel Deutschland* (2022)) that when a certain matter is regulated by EU law there is no place – unless expressly allowed - for ordinary domestic law, in particular contract law set out in civil codes. One can expect that at a certain point the Court will take this position with regard to digital euros, but it will take time.

[22] To understand the position taken by the Digital euro Regulation one should bear in mind the conclusion of the Report by the Euro Legal Tender Group, (ELTEG), 2009: «A clear majority of Group members were in favour of the principle of general acceptance of cash in B to C relationship, the refusal being the exception and always based on reasons related to the "good faith" principle. Members from four Member States however argued that contractual freedom can limit legal tender provisions (IE, DE, FI, NL)». Report by the Euro Legal Tender Group, (ELTEG), 2009, 10: «For a clear majority of members, high denomination banknotes should in principle be accepted. They can only be refused based on the "good faith" principle and/or specific national rules (e.g., "*obligation de faire l'appoint*" in FR). For 4 members, the concept of legal tender does not affect the possibility –based on contractual freedom- of the parties agreeing that payments cannot be made with high denomination banknotes. In any event, the banknotes might also be rejected on the 'good faith' principle».

[23] Unless, obviously, the payee already and normally uses other forms of digital payment: see the Digital euro Regulation, art. 9.

ii. Conversely, the obligation to make a dematerialized payment may result either from agreements or from regulatory provisions. Transposing this rich experience with reference to the digital euro, it is easy to imagine cases in which certain subjects are required to accept payment with this currency (typically in all cases in which they already accept or are required to accept electronic payments). And cases in which it is possible to pay only with digital euros or with another electronic instrument.
iii. Basically, relationships between private individuals that are not regular, or payments made by professionals to non-professionals (the typical case is that of payment in cash to the pensioner at the post office), would remain outside this framework[24].
b) The other characteristic of money having legal tender is that the payment through it extinguishes *ipso iure* the monetary obligation, at least for the amount corresponding to the payment.
This effect therefore should also occur when the payment is made with digital euros, on the basis of the principle of equivalence of the currency, be it physical or digital.
However, the fact that a payment in a digital form requires the correct functioning of technological equipment -in transmission of the order, in reception of the sum - which are beyond the control of the parties, must be considered[25]. The hypotheses of malfunctioning are multiple and obvious: the payment of an amount that the debtor does not hold in his e-wallet; the payment of an amount higher than the one ordered; failure to transmit the order; the non-crediting of the payment, or the crediting of a lower amount[26].
While with traditional cash all these unforeseen events - and the related risks - are borne by the parties, it seems reasonable to believe that - in view of the indispensable trust that a currency with legal tender must ensure - these technological risks weigh on the issuer, *i.e.* on the central bank (or on the subject indicated by the latter as an intermediary)[27].
And just as with reference to cash, the risk of theft or robbery weighs on the bearer, in the case of digital currency – excluding the (by now typified) cases of self-responsibility of the holder – the risk of theft/misappropriation of amounts should weigh

[24] Art. 9 of the Digital euro Regulation foresees an exception when «the payee is a natural person acting in the course of a purely personal or household activity».

[25] According to art. 30 of the Digital euro Regulation «Final settlement of online digital euro payment transactions shall occur at the moment of recording the transfer of the digital euros concerned from the payer to the payee in the digital euro settlement infrastructure approved by the Eurosystem». Therefore, a black-out of the infrastructure does not allow the settlement. As already pointed out by A. Di Majo, *Il diritto comunitario dei pagamenti pecuniari*, cit., when a payment is considered as a service that must be rendered this entails obligations not only on those who formally are parties of the transaction but also to those who benefit from its performance.

[26] G. Olivieri, *La rilevanza del tempo nei sistemi di pagamento*, in BBTC, 2000, 161.

[27] Recital 64 of the Digital euro Regulation «The settlement of online digital euro payment transactions should be performed in the digital euro settlement infrastructure adopted by the Eurosystem. Online digital euro payment transactions should be settled in a matter of seconds as specified under the functional and technical requirements adopted by the European Central Bank. Final settlement of online digital euro payment transactions should be achieved at the moment of recording the digital euros concerned of the payer and the payee in the digital euro settlement infrastructure approved by the European Central Bank, irrespective of whether digital euros are recorded as holding balances or units of value, or of the technology used».

on the issuer (or on his intermediary). The typical hypothesis - of which we have seen excellent and easily predictable examples with reference to the so-called crypto-currencies – is that of intrusion into the computer network with the transfer of sums in favour of subjects or entities other than the entitled person[28].

Likewise, one could posit that the issuer (or its intermediary) must bear the risk of malfunctioning of the system which makes payment impossible, with damage for the user (the failed last-minute purchase of a transport ticket; impossibility to participate in an online auction; failure to meet a tax deadline, etc.)

Almost fifty years of practical experience has taught us how to deal with and solve these cases in the world of traditional electronic payments[29].

But in such cases an entirely private law relationship is created between the payer and his credit institution; between the latter and the payee's credit institution; between the latter and the payee. Relationships which are governed by general terms and conditions and sometimes by consumer law.

The framework has not changed much - if not for an increased regulatory dimension - in cases where a third party is added to the relationship, such as the issuer of a credit or debit card.

But in the case of a CBDC it can be doubted that the relationship between the issuer (central bank) or its intermediary and the entitled person is governed by private law, and rather should not be qualified entirely under public law[30], as in the cases (which make the joy of numismatics) of banknotes printed by the central bank containing errors that prevent their use[31].

There is further point that has to be made: the role of banks in enabling the purchase, use and conversion of digital euros is entirely technical. They are not providing

[28] The cryptocurrencies fans maintain that CBDCs should use the Distributed Ledger Technology (DLT) which is notorious for been used in the Bitcoin system. Quite aptly F. Panetta in his speech, *Demystifying wholesale central bank digital currency*, 26.9.2023 notes that «central bank money has been available in digital form for wholesale transactions between banks for decades. This misconception is fuelled by the commonly held assumption that wholesale CBDC needs to be operated using DLT. But wholesale CBDC is not synonymous with DLT, as it can be based on any digital technology». Adding this important comment concerning monetary sovereignty: «Importantly, the governance of major DLT technologies and networks is dominated by actors who are either unknown or based outside Europe, which raises concerns about strategic autonomy». In the same direction see J. Cullen, *Economically inefficient and legally untenable: constitutional limitations on the introduction of central bank digital currencies,* in *Journal of Banking Regulation,* 2022, 39 «By offering a standardised and non-proprietary interoperable payments infrastructure, this might also ensure that large tech firms could not come to dominate payments markets, in effect avoiding the replacement of one set of dominant institutions by another».

[29] And one should not forget the issues of clearing houses and of netting: see M. Perassi, *Il diritto comunitario dei pagamenti*, in G. Carriero - V. Santoro, *Il diritto del sistema dei pagamenti*, cit., 141; and N. Vardi, *The Integration of European Financial Market*s, cit., 62 ss. For the situation at the dawn of digital payments see V. Zeno-Zencovich, *Clearing houses informatizzate e irrevocabilità del pagamento*, in *Diritto informazione e informatica*, 1987, 555.

[30] «No account or other contractual relationship would be established between the digital euro user and the European Central Bank or the national central banks». (Digital euro regulation, recital 9). The Digital euro Regulation aims at introducing (at art. 27) a dispute resolution mechanism for payment service providers and e-money users in the cases of technical and fraud controversies.

[31] One should recall the public law approach to money set out over a century ago by G. F. Knapp, *Staatlische Theorie des Geldes*, Berlin, 1905.

credit to the user, nor are they depositaries of the digital currency. They are simply technological enablers which record the various operations. Therefore, in the case of insolvency of the credit institution the digital euros should remain unscathed.[32] And it remains to be seen who should be responsible for errors or frauds in some way connected to the third parties providing technological services.

In conclusion, since it does not seem that private law can adequately assist the parties who have suffered damage in the use of a CBDC, its introduction must be accompanied by the necessary public regulatory interventions, which inevitably influence the law of pecuniary obligations and their exact fulfilment.

c) Finally, with regard to the digital euro, the issue of bearing interest, considered immanent in pecuniary obligations, should be considered.

If we consider cash and digital currency equivalent, the consequence is that the latter, once placed in the possession of the holder, is not interest-bearing, as happens if one has banknotes in one's wallet. Indeed, the natural fruitfulness of money presupposes that there must be a credit/debit relation between two parties and whoever disposes of the sum can make a profitable use of it. A situation quite different from that of reserve deposits of commercial banks with their central bank.

But with digital currency this is not possible, on the one hand because it is in the exclusive availability of a subject, and therefore no one else can use it. And on the other hand, the issuing institution is precisely the institutional issuer of the currency, not a subject who makes its own use of it[33].

In order for digital currency to produce interest, it is therefore necessary that it be deposited with an authorized intermediary and made available to the latter. The situation is clear when one considers the difference between the case in which a person deposits a certain amount into his bank account; and the case in which he deposits the same amount, in banknotes, in his safety deposit box.

4. Digital Euro and the GDPR

If the aspects that have been presented so far fit into the well-established province of pecuniary obligations, there are others that instead depend on regulatory factors, and therefore are variable and transitory in relation to preeminent legislative policy choices.

The first is that of the digital euro's relationship with the instable galaxy of personal data protection, which in the last years has become a pillar - if not even an obsession - of European Union law.

The intersection is due to the fact that a digital currency must necessarily be connected to an identified subject who is entitled to it and is authorized to dispose of it[34]. And

[32] And in effect the Digital euro Regulation states that «the insolvency of payment service providers would not affect digital euro users» (recital 9).

[33] Art. 16, para. 8 of the Digital euro Regulation: «the digital euro shall not bear interest».

[34] R. Lattanzi, *Sistemi di pagamento e protezione dei dati personali. Prime note*, in M. Mancini – M. Perassi (eds.), *Il nuovo quadro normativo comunitario dei servizi di pagamento. Prime Riflessioni*, Quaderni di Ricerca

this makes it possible to trace its circulation backwards and therefore the reasons/occasions of its use. In contrast, cash is anonymous, and its disintermediated circulation much more difficult to trace, in space and time.

This characteristic of cash constitutes one of its attractive and preferential elements compared to other payment instruments, including the future digital euro. Nor is it a question that can be resolved with a simple legislative *fiat*[35]. We have always known that money has its foundation in its social use, and if it is not accepted, society will move towards alternative instruments.

To try to limit the competitive disadvantage compared to cash, all the preparatory documents for the digital euro state that it will be "anonymous", like cash.

Now, it is necessary to clarify once and for all and in a *tranchant* way: in the digital universe there are no "anonymous" data. With greater or lesser deployment of resources it is possible, by cross-referencing allegedly "anonymous" data from various databases, to identify with certainty or reasonable approximation the subject to which they refer. Already the fact that a digital payment must start from a specific electronic device, through a network, to reach another electronic device or an account, also electronic, means that there are at least three databases that contain elements - time, place, nature of the impulse – which make the promise of "anonymity" purely declamatory. And this happens also, albeit in a subsequent time sequence, in the case of off-line transactions.

But there is a further element, this time regulatory, which makes the announced "anonymity" of the digital euro scarcely reliable[36].

The mammoth (and ever-expanding) General Data Protection Regulation (679/16) (the so-called GDPR) repeatedly provides (see *e.g.* articles 6 and 23) that numerous principles do not apply in the case of the exercise of public functions or the pursuit of the financial interests of the Union or of a Member State. And both the first Directive on payment systems (art. 79) and the PSD2 (art. 94[37]) provide for the processing of personal data pursuant to the law to prevent and combat cases of fraud. It is therefore foreseeable that the veil of the declaimed anonymisation of transactions in digital euros will, at law and in fact, be pierced by a number of exceptions making it

Giuridica della Banca d'Italia n.63, December 2008, 161.

[35] See recital 16 of the Digital euro Regulation: «The mandatory acceptance of payments in digital euro as one of the main conditions of the legal tender status ensures that people and businesses benefit from a wide acceptance and have a real choice to pay with central bank money in a digital way and in a uniform manner throughout the euro area».

[36] V. Santoro, *Considerazioni sulla moneta*, in *Diritto della Banca e dei Mercati Finanziari,* 2022, 185 points out that «anonimity is a notion quite different from that of privacy». And the ECB, in the Monthly Bolletin Report, 29.9.2002, states «Full anonymity is not considered a viable option from a public policy perspective».

[37] «Member States shall permit processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation and detection of payment fraud. The provision of information to individuals about the processing of personal data and the processing of such personal data and any other processing of personal data for the purposes of this Directive shall be carried out in accordance with Directive 95/46/EC, the national rules which transpose Directive 95/46/EC and with Regulation (EC) No 45/2001».

transparent[38].

However, this conclusion should not come as a surprise. In the digital universe of every event there remains a trace and therefore it can be reconstructed. This already occurs eminently for payment systems which, due to their importance, require identification, certainties, durable supports and high security networks; and to all this it should be added that since a multiplicity of legal effects are connected to each payment - not only in the field of private law, but also and above all in that of public/administrative/tax law - the memorization and traceability of all these factors constitutes a *sine qua non* condition. The digital euro, therefore, in this respect, does not differ from the other common forms of electronic payment to which we have long been accustomed, without the transparency of the transactions having hindered their diffusion and prevalence[39].

If anything, the operation that - adopting a fashionable expression - could be defined as "privacy-washing" has the function of reassuring the public of an equivalence that in reality does not exist: in the "analogue" world, payments by cash present some grey areas, which are dissolved in the digital one.

With these lenses one can read with a certain scepticism Chapter VIII of the Digital euro Regulation devoted to "Privacy and data protection" and which includes articles from 34 to 36 and whose aim is to pass muster with the EDPS[40] and eventually the EUCJ.

---

[38] In the first place there is a preliminary need to verify and match the identity of digital euro holders. See recital 25 of the Digital euro Regulation: «For the purpose of properly enforcing any holding limits on the use of the digital euro decided upon by the European Central Bank, when onboarding digital euro users, or during ex-post checks where appropriate, payment service providers in charge of distributing the digital euro should verify whether their prospective or existing customer already has digital euro payment accounts». And quite naturally, art. 32 of the Digital euro Regulation introduces a «general fraud detection and prevention mechanism». Although its para. 4 states that the measures «shall not be able to directly identify the digital euro users on the basis of the information provided to the fraud detection and prevention mechanism», it is clear that once a fraud is suspected identification will subsequently follow. The ECB documents cautiously place themselves on the line of "data minimization" (art. 5, para. 1, letter c), GDPR): «As approved by the Governing Council, the Eurosystem is committed to provide for highest levels of privacy within the regulatory framework. The Eurosystem has no interest in exploiting individual payment data for any purpose. This stands in contrast to the monetisation of individual payment data by private companies. The availability of data visible to the Eurosystem will be limited to only that what is necessary to perform its tasks or is required by regulation. To this end, the digital euro solution shall be designed in a way that aims to minimise the Eurosystem's involvement in the processing of users' data».

[39] A research by the Bank of Korea on a sample of 3500 Korean citizens points out that there would be a preference towards CBDC – in respect of other forms of digital payment – if a higher level of privacy were ensured for the purchase of sensitive goods and services such as mental health-care or adult products but «in the situation of purchasing privacy-insensitive products (e.g. food, office supplies),we find negligible treatment effects in both offline and online purchasing situations». S. Choi et al., *Central Bank Digital Currency and Privacy: A Randomized Survey Experiment*, 2022, 4.

[40] The EDPS in Press and Publication about "Tecnosar" has already expressed himself in these terms on the risks presented by CBDCs: «Concentration of data in the hands of central banks could lead to increased privacy risks for citizens: if payment data of all citizens were concentrated in the databases of a central bank, it would generate incentives for cyberattacks and a high systemic risk of individual or generalised surveillance in case of data breaches or, more in general, of unlawful access.
- Wrong design choices might worsen data protection issues in digital payments: payment data already reveals very sensitive aspects of a person. Wrong design choices in the underlying technological infrastructure might exacerbate the privacy and data protection issues that already exists in the digital payment landscape. For example, transactional data could be unlawfully used for credit evaluation and

5. Regulatory Limits on the Use of CBDCs

Another normatively variable factor is given by the limits that one can expect will be imposed on the use of the digital euro. In the various preparatory documents, maximum amounts are mentioned between €3,000.00 and €5,000.00[41]. Above these ceilings, the surplus would be transferred automatically to the holder's bank account[42]. Therefore, the possibility - worrying in terms of monetary supervision by the central bank - of hoarding huge resources in the form of digital euros must be excluded[43]. And at the same time, it must be emphasized that this limit cannot be justified by purposes of contrasting tax evasion or money laundering. In fact - as pointed out in the previous paragraph – digital payments, unlike those through banknotes and coins, are always traceable, especially when, due to their amount and the circumstances in which they are made, they fall under the attentive control of automatic monitoring programs.

In any case, the immaterial and technological nature of digital money requires that - unlike cash - there is, upstream, a private law contract with a credit institution. The provision of digital euros will therefore be a new service offered to its customers[44], who in some cases - typically commercial establishments - will be required to use it

cross-selling initiatives.

- Lack of security might turn into severe lack of trust from users: security concerns in the CBDC infrastructure, whose security requirements and expectations are high, may turn into a significant loss of trust from users» (EDPS, Tech Dispatch, 1/2023, 29.3.2023).

41 P. Wierts - H. Boven, *Central bank digital currency – Objectives, preconditions and design choices*, De Nederlandsche Bank Occasional Studies, 2020, 36 ss.

The Digital euro Regulation (art. 16) leaves it to the ECB to establish the «limits to the use of the digital euro as a store of value».

42 The so-called "waterfall functionality" described in recital 36 of the Digital euro Regulation which follows the Report Progress on the investigation phase of a digital euro, 29.9.2022: «Quantitative limits on digital euro holdings of individual users could limit individual take-up and the speed at which bank deposits are converted into digital euro». Additional functionalities could avoid negative effects of holding limits on user experience. One such tool could be the "waterfall" functionality, under which funds in excess of the digital euro holding limit would be transferred automatically to a linked commercial bank account».

43 «The issuance of a digital euro could have the (unintended) side effect of creating competition with commercial bank deposits, as households and companies may consider the digital euro an alternative to deposits rather than to cash. Faced with the risk of outflowing retail deposits, commercial banks would encounter higher funding costs—either by offering a better value proposition to their depositors or by turning to more expensive (and potentially less stable) wholesale funding markets. Moreover, they would be obliged to adapt their business models to the 'new reality' of a diminished deposit base, with still uncertain effects on the economy at large. Arguably, however, the greatest risk to financial stability stems from the fact that a digital euro would facilitate a flight from commercial bank deposits to the safety of central bank money in a distressed market environment ('digital runs')». S. Grünewald - C. Zellweger-Gutknecht - B. Geva, *Digital Euro and ECB Powers*, cit. This concern underlies the whole ECB Paper "*Central bank digital currency and bank intermediation*". A concern which is common to the Federal Reserve: «Central bank liquidity may be insufficient to stave off large outflows of commercial bank deposits into CBDC in the event of financial panic». These indications are followed by recital 32 of the Digital euro Regulation states that «An unrestricted use of digital euro as a store of value could endanger financial stability in the euro area, with adverse effects on credit provision to the economy by credit institutions».

44 T. Ahnert *et al.*, *The economics of central bank digital currency,* in European Central Bank Working Paper, August 2022.

by virtue of the legal tender principle of the digital euro. The difference compared to common debit/credit cards is obvious: with reference to the latter, there is an intermediary who, in exchange for a fee, assures the cardholder the possibility to pay almost everywhere, immediately, without having to carry cash (or various types of currencies). And to the payee the solvency of the debtor and direct credit procedures on his own account.

The digital euro therefore is clearly distinguishable from the rather unsatisfactory experience of e-money, with which an attempt was made to create alternative payment circuits to debit/credit cards[45]. With e-money, the subject paid or withdrew an amount and received an equivalent credit to spend within certain circuits that accepted it. To the contrary digital euro is not a credit towards a private entity; there is no conversion of legal tender into a credit that can be spent only with certain subjects belonging to a circuit; it is not "refundable"[46]. But above all it cannot have a cost. In fact, if a fee had to be paid to acquire digital euros (To whom? To the issuing institution?) not only from an economic-social point of view the endeavour would die even before being born, but above all it would challenge, at its root, the nominalistic principle: *Mark gleich Mark*. One euro – physical or digital – is worth one euro, always material or digital[47]. What may have a cost - but it is foreseeable that it will be included in that of the connected current account[48] - is the "digital cash" service, which however is a relationship external to the supply and availability of digital euros.

This conclusion appears to be consistent with the "ceiling" on the availability of digital euros, within the limits indicated above. These are amounts that imply a prevailing use of digital euros *ex parte creditoris*, in B2C or C2C relationships. The professional *accipiens* of the digital euro will make modest use of it for micro-payments[49], the more common ones being entrusted to normal commercial practices - especially as to their

[45] Directives 2000/28 and 2000/46 had introduced a detailed regulation of e-money. S. Sica - P. Stanzione - V. Zeno-Zencovich (eds.), *La moneta elettronica: profili giuridici e problematiche applicative*, Milan, 2006.The most notable case is that of PayPal which has had considerable success. It is doubtful, however, that it has created an effective competition with the major credit card companies.

[46] Recital 66 of the Digital euro Regulation makes this clear: «Payment service providers are not party to a digital euro payment transaction between two digital euro users».

[47] Nearly 15 years ago these were the conclusions of the ELTEG Report: «The majority of Group members felt that: a) no surcharges (either express or by measures of equivalent effect on all other available means of payment) can be imposed on payment through the use of the legal tender currency, euro banknotes and coins; and b) Surcharges can be imposed on other means of payment, the mere existence of *pouvoir libératoire* not attributing to them the quality of legal tender. Members from five Member States (IE, DE, FI, NL, SI) considered that the imposition of cash surcharges was legally permissible and did not necessarily conflict with the legal tender status of currency». And, in fact, recital 41 of the Digital euro Regulation states that «The European Central Bank or the Eurosystem do not charge payment service providers for the costs it bears to support their provision of digital euro services to digital euro users».

[48] J. Cullen, *Economically inefficient and legally untenable: constitutional limitations on the introduction of central bank digital currencies,* cit.: «Because banks may offer bundled products alongside payment services, they can cross-subsidise their payments services and infrastructure costs and there are well-established findings that banks and other financial institutions with direct access to central bank settlement systems enjoy competitive rents from these privileges».

[49] The Digital euro Regulation states, from the beginning, that «the digital euro should support a variety of use cases of retail payments» (recital 4).

scheduling - through bank orders[50].
The use of the digital euro therefore appears to be placed, in general, within the complex and hyper-regulated system of consumer law. It follows that the payment by the consumer with the means of digital euros will have to enjoy the same protections normally offered both for distance contracts (especially the right to reconsider and of withdrawal), and for payments made through debit/credit cards. In this last field one disposes of over thirty years of regulations and case-law aimed at protecting the user. One should ask oneself if they could be extended to the user of the digital euro. The reply requires careful examination of the many implications, taking into account the kind of relationship that is created by the use of digital euros. In any case, however, an *ad hoc* regulatory intervention would be necessary.

6. Digital Euro as a Platform

More generally, the advent of the digital euro means that the relationship between issuer and user is placed in a different context than the "analogue" one of cash[51]. Previously, the risks deriving from malfunctioning of electronic equipment or networks, and those from digital intrusions and misappropriations have already been highlighted. Once upon a time, the issuer's role ended with the printing/minting and distribution of banknotes or metal coins. After this activity there were those related to the deterioration of the material object (withdrawal of banknotes damaged or replaced by a new design) and the fight against counterfeiting. In the world of the digital euro, the circulation of money is under constant supervision, which implies a continuity of legal relations between the issuer and the holder of the money.
One has already pointed out that the introduction of the digital euro fits into a political and geopolitical context specific to every monetary decision[52]. This is not the place to analyse the multiple and complex aspects that go beyond private law relationships and pertain to public law and international law and politics.
However, some comments must be made:
a) In economically evolved societies with predominantly consumer-driven models (in simple terms: the reduction in consumption is reflected on the entire economy with recessive chain effects) money is an essential factor of citizenship. Although it is a highly debatable tendency, the position of each citizen and the theoretical equality between them is increasingly measured in terms of consumption capacity, of which

[50] Again, the same recital states that «The digital euro should not cater for payments between financial intermediaries, payment service providers and other market participants (that is to say wholesale payments)».

[51] A. Di Majo, *Il diritto comunitario dei pagamenti pecuniary,* cit. already pointed out the immense distance between the domestic rules governing the discharge of pecuniary obligations and the EU systems of payments which covers not only debts in euros but also in other currencies of Member States or of the EEA.

[52] S. Grünewald - C. Zellweger-Gutknecht - B. Geva, *Digital Euro and ECB Powers,* cit., «digital banknotes must be designed as a functional equivalent to tangible banknotes. Accordingly, their functions must be limited to those of a means of payment and a store of value, excluding their use as a monetary policy instrument».

money is the prerequisite[53].

The digital euro must be available in an "inclusive" way[54] not only by avoiding the creation of a further "digital divide", or effects of stigmatisation/exclusion of those who do not adapt to more technologically advanced models[55].

One of the corollaries is that the cost of introducing the digital euro - which, as we have seen, is intended to be used as a means of payment mainly by consumers - cannot be borne by the latter through opaque "price transfer" procedures[56]. The obvious parallel is with consumption taxes, which are notoriously regressive in their nature. Therefore, the regulation – even by private law – of the digital euro cannot ignore this dimension and the social implications of public choices.

b) The second broader profile that must be examined concerns the natural global dimension of digital phenomena, as everyone can see in the use of ubiquitous online services, raising the question of the territoriality of the new digital currency. The Dig-

[53] On the "class" nature of money both in ancient and present times see V. Santoro, *Considerazioni sulla moneta,* cit., 185 ss.

[54] See L. Galotto - M.I. Vangelisti, *Designing an inclusive digital euro*, in 16 *J. Payments Strategy & Systems*, n°. 2, 137 (2022).

[55] The issue is considered already in the Legal tender Regulation with regards to cash payments: «financially excluded people, such as the unbanked, asylum seekers and migrants, who may not be able or willing to use means of payment supplied by the private sector, rely on cash as their payment method. Cash is considered to provide for a clear overview of expenses, with high degrees of ease of use, speed, safety and privacy». (recital 14) The rule is expressed in art. 8 (Access to cash): «Member States shall ensure sufficient and effective access to cash throughout their territory, in all their different regions, including urban and non-urban areas». And the Digital euro Regulation states that «it is essential to support financial inclusion by ensuring universal, affordable and easy access to the digital euro to individuals in the euro area, as well as its wide acceptance in payments. Financial exclusion in the digitalised economy may increase as private digital means of payments may not specifically cater for vulnerable groups of the society or may not be suitable in some rural or remote areas without a (stable) communication network». (recital 5). The text reflects what had been written by S. Grünewald - C. Zellweger-Gutknecht - B. Geva, Digital *Euro and ECB Powers,* cit.: «By providing costless access to a simple, universally accepted, credit risk-free, and trusted means of payment and store of value, the euro represents an important public good for European citizens». See also J. Cullen, *Economically inefficient and legally untenable: constitutional limitations on the introduction of central bank digital currencies,* cit.: «A CBDC would be highly beneficial for low-income households, which tend to rely heavily on cash and whose access to bank accounts may be limited. Small businesses, who are often charged large account and transaction fees, and must contend with additional charges for accepting debit and credit card payments would also benefit from the introduction of a CBDC».

[56] There is a growing tendency by public entities to impose, as only form of payment, digital procedures which bear a cost in favour of intermediaries which often are publicly owned companies. The result is that the debtor must "pay to pay". While this is not allowed in B2C relationship, in this case the payer is not considered a consumer. The ECJ has taken a rather pharisaic position in the ECJ, C-422/19, *Dietrich c. Hessischer Rundfunk* (2021), widely cited in the two proposed Regulations: art. 128 TFUE «must be interpreted as not precluding national legislation which excludes the possibility of discharging a statutorily imposed payment obligation in banknotes denominated in euro, provided (i) that that legislation does not have the object or effect of establishing legal rules governing the status of legal tender of such banknotes; (ii) that it does not lead, in law or in fact, to abolition of those banknotes, in particular by calling into question the possibility, as a general rule, of discharging a payment obligation in cash; (iii) that it has been adopted for reasons of public interest; (iv) that the limitation on payments in cash which the legislation entails is appropriate for attaining the public interest objective pursued; and (v) that it does not go beyond what is necessary in order to achieve that objective, in that other lawful means of discharging the payment obligation are available». Clearly, in the case of payments in digital euros all the excuses made by public authorities to refuse payments in cash fall through.

ital euro Regulation tries to set a few limitations, stating (art. 8) that «The digital euro shall have legal tender status for online payments of a monetary debt denominated in euro to a payee residing or established in the euro area». Therefore, imagining the typical online transaction, extra EU providers of goods or services must establish themselves in the Union if they want to take advantage of being paid directly in digital euros. Art. 18 of the same Regulation states that «Payment service providers may only distribute the digital euro to natural and legal persons residing or established in a Member State whose currency is not the euro if the European Central Bank and the national central bank of that Member State have signed an arrangement to that effect». And art. 19 sets higher standards for possible agreements between the ECB and third countries. These limitations – whose aim is self-evident (and laid out in the recitals) – remind us of the still common restrictions one finds in many countries to the use of domestic currencies by foreigners: one may not import or export domestic banknotes; foreign currency must be exchanged in local currency in official change bureaus. It remains to be seen how the envisaged e-monetary protectionism will fare in global money markets and networks.

c) Always in transnational perspective one should consider that if the cost of the digital currency is zero, the advantage of using the digital euro from countries outside the Eurozone (both EU and non-EU) is immediate as it is free from onerous exchange rates and commissions imposed on every transaction. And, of course, the reverse is true, assuming that other countries – the most obvious example is the United States[57] – digitize their currency. This implies that it would be highly convenient for a person, natural or legal, to hold multiple e-wallets in the most used currencies (*e.g.* US dollar, British pound, Swiss franc). However, as one has seen, the Digital euro Regulation allows such a practice only on the basis and at the conditions set out in a specific bilateral agreement.

d) The introduction of the digital euro should lead to a significant reduction in the payment/collection costs currently carried out by electronic means. In the case of the most common transactions through debit/credit cards there generally is a fixed annual fee for the holder of the card; and for the commercial payee a fixed or percentage commission for each operation, to which one must add a fee for the technical validation equipment and for the connection to the network. These are amounts that overall reach very high volumes, to a large extent appropriated by non-EU financial entities (such as VISA, MasterCard or American Express)[58]. In addition to the - very important - issue of monetary sovereignty[59], the digital euro can - and should, if it is to be successful -

[57] Which are well aware of the same issues as explained in Report of the Federal Reserve Money and Payments: The U.S. Dollar in the Age of Digital Transformation, January 2022: «The potential for significant foreign demand for CBDC would further complicate monetary policy implementation».

[58] And one should add the extraordinary economic and strategic value of the collection, storage and processing of financial data (even without raising the issue of transborder transfers of personal data). The issue, with regards to the SWIFT system, has been the object of Opinion 10/2006 of the Article 29 European Data Protection group.

[59] Repeatedly mentioned in the Digital euro Regulation at recitals 38 and 47, and in its "explanatory memorandum". The ECB has made the point in a rather elliptical way: «A digital euro would also contribute to Europe's strategic autonomy and economic efficiency by offering a European means of payment that could be used for any digital payment, would meet Europe's societal objectives and would

imply the elimination of intermediation costs, with microeconomic effects[60]. Again, one should point out that in the case of credit/debit cards the issuer guarantees both the payer and the payee that the payment is correct and that the funds are available. But in the case of a payment in a digital currency this guarantee is *per se* in the nature of money. The bank is not guaranteeing that the funds are available very simply because they are already "tagged" to an individual and can be spent only by him. The costs therefore should be minimal.

e) With its digital currency the State enters in direct competition with private entities to govern modern payment systems[61]. From a systematic point of view, the digital euro is not just a legal tender: it constitutes a platform in the sense that computer science and socio-economic theories ascribe to it. A multiplicity of subjects – credit institutions, companies, public administrations, private citizens – access, communicate, exchange and regulate relationships through this platform. Whoever issues the digital currency therefore has a direct, constant and global control over the platform and therefore takes on functions that are specific to digital networks and relationships[62]. This determines an inevitable metamorphosis of central banks in their role as issuing institution, and will entail, in the governance of money, a growing importance of decision-making mechanisms typical of the digital world (big data, user profiling, predictive analytics, artificial intelligence). Over the past years and presently a great deal of debate is ongoing concerning the role of private platforms as political actors governing social and economic processes. Much less attention has been, instead, devoted to the changing role of "government as platform". This already happens in significant areas of our welfare state (education, health, social security). Now is the turn of monetary policies. This perspective must also be kept in mind when shaping the law of digital pecuniary obligations.

be based on a European infrastructure».

[60] The Digital euro Regulation proposes (art. 17) that the charge for transactions in digital euros should not exceed the lowest between the fees requested for comparable means of digital payment (*viz.* credit/debit card) or the relevant cost incurred by payment service providers for the provision of the service including a reasonable margin of profit. While the former are set in accordance with Regulation (EU) 2015/751 on interchange fees for card-based payment transactions, the latter are more complex to establish. The ECB TIPS (immediate payment system) sets a € 0.002 fee per transaction. From January 2024 this fee should be equally shared between payer and payee. How do these provisions combine with the principle stated in recital 40: «To ensure wide access to and use of the digital euro, consistent with its status of legal tender, and to support its role as monetary anchor in the euro area, natural persons residing in the euro area (…) should not be charged for basic digital euro payment services»? The response lies in recital 45: «an inter-PSP fee may be needed to provide compensation to those payment service providers for the distribution costs». On the "basic" services envisaged by the PSD Directives see A. Sciarrone Alibrandi, *L'adempimento dell'obbligazione pecuniaria tra diritto vivente e portata regolatoria indiretta della Payment Services Directive 2007/64/CE*, in M. Mancini - M. Perassi, *Il nuovo quadro normativo comunitario dei servizi di pagamento. Prime Riflessioni*, Quaderni di Ricerca Giuridica della Banca d'Italia n.63, cit.

[61] As J. Cullen, *Economically inefficient and legally untenable: constitutional limitations on the introduction of central bank digital currencies,* cit., notes the EU has, until now, failed in trying to introduce payment systems alternative to traditional bank transfers or credit/debit cards.

[62] On this new and different notion of monetary sovereignty see S. Murau - J. Van't Klooster, *Rethinking Monetary Sovereignty: The Global Credit Money System and the State*, in *Perspectives on Politics*, 1, 2022. But, to the contrary, see C.D. Zimmerman, *The Concept of Monetary Sovereignty Revisited*, in *European Journal of International Law*, 2013, 818: «the concept of monetary sovereignty cannot, by its very nature, become eroded under the increasingly strong impact of various economic and legal constraints».

Dal "caso Casapound" del 2019 alla "sentenza Casapound" del 2022: piattaforme digitali, libertà d'espressione e odio *on line* nella giurisprudenza italiana*

Giulio Enea Vigevani

Abstract

L'articolo prova a offrire un quadro sistematico delle tendenze della giurisprudenza italiana, nei casi relativi alla rimozione da parte dei social media di pagine o account di movimenti politici, a causa della presenza in essi di contenuti d'odio. L'autore individua tre orientamenti giurisprudenziali, differenti non solo nell'esito ma anche nell'interpretazione di quale sia la natura giuridica di una piattaforma, quali limiti incontri nella definizione delle condizioni contrattuali, quale sia il rapporto tra esercizio delle libertà politiche e social network, quali diritti gli utenti (e specie le formazioni politiche) possano vantare nei suoi confronti e quale sia lo spazio di intervento dei pubblici poteri nella sua regolazione. In ultimo, l'autore prova a prospettare alcune strategie che consentano, alla luce dei principi del costituzionalismo classico e della normativa europea, di limitare i discorsi d'odio ponendo al contempo un freno al potere di cui godono le principali piattaforme digitali.

The essay attempts to offer a systematic overview of the trends in Italian jurisprudence, in cases related to the removal by social media of pages or accounts of political movements, due to the presence of hateful content in them. The author identifies three jurisprudential orientations, differing not only in the outcome but also in the interpretation of what is the legal nature of a platform, what limits it encounters in the definition of contractual conditions, what is the relationship between the exercise of political freedoms and social networks, what rights users (and especially political groups) can claim against it, and what is the space is available for public authorities to intervene in its regulation. Finally, the author tries to outline some strategies that would allow, in light of the principles of classical constitutionalism and European law, to limit hate speech while curbing the power enjoyed by major digital platforms.

* Questo scritto è destinato al volume "*Libertà di espressione al tempo dei social media*", a cura di Ginevra Cerrina Feroni e Edoardo C. Raffiotta, di prossima pubblicazione da parte della Casa editrice Il Mulino nella Collana "Studi e ricerche Cesifin. Su determinazione della direzione, ai sensi dell'art. 15 del Regolamento, il contributo non è stato sottoposto a referaggio

Giulio Enea Vigevani

Sommario

Keywords

libertà di espressione – libertà di associazione - piattaforme digitali – moderazione contenuti *online* - movimenti neofascisti

1. L'oscuramento degli *account* di movimenti neofascisti, tra libertà di espressione, libertà contrattuale e difesa della democrazia

Il diritto dell'informazione in rete rappresenta da tempo un territorio ove emergono continuamente questioni che investono alcuni grandi temi del costituzionalismo contemporaneo: le regole del libero confronto delle idee nella sfera pubblica, lo spazio per le "parole pericolose", la tutela della dignità delle persone e dei gruppi, il rapporto tra autorità statali, poteri privati e cittadini, la concezione stessa della democrazia.

Tali questioni si manifestano soprattutto nelle aule di giustizia, in ragione della difficoltà del legislatore, europeo e italiano, di intercettare tempestivamente i temi che l'evoluzione tecnologica pone al mondo del diritto.

Così, accade di frequente che sia demandata alle corti, nazionali e sovranazionali, la risoluzione di controversie "nuove", senza che il legislatore abbia predisposto coordinate normative chiare. E succede spesso poi che la risposta di un giudice a un singolo caso finisca agli occhi dell'opinione pubblica con l'identificarsi con la regola generale in quella materia. Ciò avviene talvolta per ragioni che poco hanno a che vedere con l'autorità dell'organo decidente o con il rigore del ragionamento giuridico ma semmai per la novità delle questioni e per il clamore mediatico del caso concreto.

Ciò è accaduto, ad esempio, con l'ordinanza cautelare del 12 dicembre 2019 del Tribunale di Roma[1], che ordinava a Facebook di riattivare la pagina di Casapound e il profilo di un suo dirigente, oscurati pochi mesi prima dal *social network* senza inviare alcuna comunicazione e senza esplicitare le motivazioni, per violazione delle condizioni d'uso, che vietano di veicolare messaggi d'odio o di incitamento razziale. Si tratta,

[1] Trib. Roma, sez. spec. imprese, ord. 12 dicembre 2019, confermata, sia pure con una motivazione diversa, in sede di reclamo (Trib. Roma., sez. civ. XVII, ord. 29 aprile 2020).

invero, di una decisione poi revocata dal Tribunale all'esito del giudizio di primo grado[2] e peraltro rimasta sostanzialmente isolata, in un panorama giurisprudenziale ormai piuttosto ampio. Tuttavia, tale pronuncia ha avuto una straordinaria eco nei mezzi di comunicazione, nonostante la presenza di decisioni coeve che andavano in direzione opposta[3] e nonostante gli appelli alla prudenza dei primi commentatori, fossero essi tendenzialmente adesivi[4] o critici[5] rispetto alla ricostruzione dogmatica del tribunale romano.

In questa prospettiva, può essere di qualche utilità offrire un quadro sistematico delle tendenze della giurisprudenza italiana, nei casi relativi alla disabilitazione da parte dei *social media* di *account* o alla rimozione di pagine aventi contenuto *lato sensu* politico. Negli ultimi tempi, infatti, vi è stata una alluvione di pronunce, da parte dei giudici di merito civili, derivanti principalmente da ricorsi cautelari di individui o associazioni che richiedono il reinserimento di contenuti rimossi o la riattivazione di account bloccati o sospesi da parte di una piattaforma digitale.

Infatti, accade di frequente che un *social network* provveda a oscurare pagine e profili di singoli o di movimenti, spesso riconducibili alla galassia della destra neo-fascista, in ragione della presenza negli stessi di contenuti d'odio. Gli utenti solitamente invocano l'inadempimento contrattuale da parte della piattaforma e insieme la lesione di un diritto costituzionalmente garantito, la libertà di espressione e, in taluni casi, anche la libertà di associazione politica.

Le risposte della giurisprudenza sono, come emergerà di seguito, assai eterogenee non solo nell'esito ma anche nell'interpretazione di quale sia la natura giuridica di una piattaforma, quali limiti incontri nella definizione delle condizioni contrattuali sull'uso dei relativi servizi, quale sia il rapporto tra esercizio delle libertà politiche e *social network*, quali diritti gli utenti (e specie le formazioni politiche) possano vantare nei suoi confronti e quale sia lo spazio di intervento dei pubblici poteri nella sua regolazione.

Si tratta evidentemente di grandi questioni, che intersecano temi centrali del dibattito costituzionalistico, quali il rapporto tra poteri pubblici e privati e tra questi e i cittadini; ciò spiega l'ampio e vivace dibattito dottrinale che ha accompagnato l'evoluzione giurisprudenziale[6].

---

[2] Trib. Roma, sez. dir. della persona, sent. 5 dicembre 2022, n. 17909.

[3] Trib. Roma, sez. dir. della persona, ord. 23 febbraio 2020, confermata in sede di reclamo, relativa alla disattivazione dei profili degli amministratori di numerose pagine riconducibili alle diverse articolazioni di un altro movimento di ispirazione neofascista, Forza Nuova; Trib. Siena, sez. un. civ., ord. 19 gennaio 2020, relativa alla chiusura di un account Facebook di un singolo, per le espressioni razziste e omofobe ivi contenute.

[4] Cfr. O. Grandinetti, *Facebook vs. CasaPound e Forza Nuova, ovvero la disattivazione di pagine social e le insidie della disciplina multilivello dei diritti fondamentali*, in questa *Rivista*, 4, 2021, 173 ss.; C. Caruso, *La libertà di espressione presa sul serio. Casa Pound c. Facebook, atto I*, in *SIDIBlog*, 20 gennaio 2020.

[5] Cfr. P. Villaschi, *Facebook come la RAI?: note a margine dell'ordinanza del Tribunale di Roma del 12.12.2019 sul caso CasaPound c. Facebook*, in *Osservatorio Costituzionale*, 2, 2020, 430 ss.; P. De Sena-M. Castellaneta, *La libertà di espressione e le norme internazionali, ed europee, prese sul serio: sempre su CasaPound c. Facebook*, in *SIDIBlog*, 20 gennaio 2020.

[6] Senza pretesa di completezza, oltre agli scritti già citati, G. M. Riccio, *La giurisprudenza su Facebook / Casa Pound e l'esigenza di eteroregolazione del contratto con il social network*, in P. Stanzione (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, 2022, 339 ss.; A. Venanzoni, *Pluralismo politico e valore di spazio di dibattito pubblico della piattaforma social Facebook: la vicenda CasaPound*, in *Diritto di*

In particolare, sul lato delle piattaforme digitali, impone di interrogarsi sull'inquadramento giuridico dei *social media*: sono servizi pubblici che possono pertanto essere assoggettati a una regolamentazione più stringente, *essential facilities* rispetto all'esercizio dei diritti individuali quali la libertà di parola e di associazione? O sono, invece, soggetti privati i cui rapporti con gli utenti sono regolati dalla normativa contrattuale, sia pure corretta a causa della diversità delle posizioni? E come incide questa qualificazione sugli obblighi di moderazione dei contenuti in capo alle piattaforme e sul loro ruolo nella sfera pubblica, nonché sul dovere in capo allo Stato di garantire effettivamente la libertà di espressione ed il pluralismo politico e informativo?

Sul lato dei diritti dei cittadini, queste decisioni ripropongono il tema dell'applicazione "orizzontale" delle disposizioni costituzionali a rapporti tra privati: sussiste davvero un diritto di tutti (o almeno di taluni soggetti qualificati) di esprimere il proprio pensiero tramite i *social media*, un "diritto al mezzo"? Ed entro quali limiti gli "standard della *community*" possano giustificare la rimozione di contenuti contrari alle regole delle piattaforme ma leciti per l'ordinamento statale?

Ancora, come incide una qualificazione pubblicistica delle piattaforme nel rapporto tra poteri pubblici e poteri privati? Quale concezione della democrazia ("aperta" o "protetta") deve essere accolta nel "mondo nuovo" della comunicazione digitale? E come può influire su tale opzione la prospettiva, in buona parte diversa, assunta dalla Costituzione italiana e dall'Unione europea nei confronti di coloro che rifiutano i valori alla base degli ordinamenti democratici?

Le risposte a tali interrogativi si riflettono evidentemente sulle argomentazioni e sugli esiti delle controversie. E, nei casi decisi dai tribunali italiani, si tratta di risposte assai differenziate, talvolta con un alto tasso di creatività, che provo a riassumere raggruppandole in tre diversi orientamenti.

Internet, 12 dicembre 2019; I. M. Lo Presti, *CasaPound, Forza Nuova e* Facebook. *Considerazioni a margine delle recenti ordinanze cautelari e questioni aperte circa la relazione tra partiti politici e* social network, in *Forum di Quaderni costituzionali,* 2, 2020, 924 ss.; B. Mazzolai, *La censura su piattaforme digitali private: il caso "Casa Pound c. Facebook"*, in *Il Diritto dell'informazione e dell'informatica*, 36(1), 2020, 109 ss.; Id., *"Hate speech" e comportamenti d'odio in rete: il caso "Forza Nuova c. Facebook*", in *Il Diritto dell'informazione e dell'informatica*, 36(3), 2020, 581 ss.; S. Piva, *Facebook è un servizio pubblico? La controversia su CasaPound risolleva la quaestio dell'inquadramento giuridico dei social network*, in *Dirittifondamentali.it*, 2, 2020; F. Pallante, *La propaganda nazi-fascista via social network e la Costituzione democratica antifascista*, in *Questione Giustizia*, 20 gennaio 2020; P. Zicchittu*, I movimenti "antisistema" nell'agorà digitale: alcune tendenze recenti*, in *Consulta online*, 5 marzo 2020; M.E. Bucalo, *La libertà di espressione in rete fra content moderation dei social network e regolazione dell'Unione Europea*, in *Dirittifondamentali.it*, 3, 2022, 270 ss.; G. Cerrina Feroni-A. Gatti, *Online Hate Speech and the Role of Digital Platforms: What Are the Prospects for Freedom of Expression?*, in C. Blanco de Morais-G. Ferreira Mendes-T. Vesting, (eds.), *The Rule of Law in Cyberspace*, Cham, 2022, 261 ss.; O. Grandinetti, *Le piattaforme digitali come "poteri privati" e la censura online*, in *Rivista italiana di informatica e diritto*, 1, 2022, 175 ss.; P. Falletta, *Analisi normativa in tema di contrasto agli hate speech su Internet e i social media*, in *H-erme. Journal of Communication*, 23, 2023, 23 ss.; G. Vasino, *Censura "privata" e contrasto all'*hate speech *nell'era delle* Internet Platforms, in *Federalismi.it*, 4, 2023, 130 ss.

2. L'approccio libertario: i *social media* sono agorà pubbliche, con l'obbligo, a tutela del pluralismo, di dar voce agli utenti e, in particolare, a tutti i protagonisti del dibattito pubblico

L'ordinanza del tribunale di Roma del 12 dicembre 2019 nella vicenda "Casapound" rappresenta il più compiuto esempio - in verità praticamente l'unico - di un orientamento che fa discendere dalla "speciale posizione" della piattaforma Facebook obblighi non dissimili a quelli tipici dei media di servizio pubblico.

In tale provvedimento cautelare il Tribunale di Roma ordinava a Facebook di riattivare la pagina di Casapound e il profilo di un suo dirigente, evidenziando «il rilievo preminente assunto dal servizio di Facebook (o di altri *social network* ad esso collegati) con riferimento all'attuazione di principi cardine essenziali dell'ordinamento come quello del pluralismo dei partiti politici (49 Cost.), al punto che il soggetto che non è presente su F. è di fatto escluso (o fortemente limitato) dal dibattito politico italiano»[7]. Di qui, il «ruolo centrale e di primaria importanza»[8] di Facebook, che attribuisce al suo gestore una «speciale posizione»[9], la quale comporta che «nella contrattazione con gli utenti, debba strettamente attenersi al rispetto dei principi costituzionali e ordinamentali finché non si dimostri (con accertamento da compiere attraverso una fase a cognizione piena) la loro violazione da parte dell'utente»[10].

Dunque, secondo questa ricostruzione, la piattaforma non può imporre misure che siano in contrasto con la libertà di manifestazione del pensiero e di associazione, eccedenti rispetto a quelli che il legislatore stesso si è dato con la normativa penale e che possano pregiudicare il diritto delle forze politiche di partecipare pienamente al dibattito pubblico attraverso i più diffusi mezzi di comunicazione[11]. In altri termini, il giudice apre a una qualificazione della natura giuridica dei servizi svolti dai *social network* come attività di interesse pubblico[12] e in capo alle piattaforme sorgerebbero obblighi di "pluralismo interno" analoghi a quelli previsti per i media di servizio pubblico.

Di qui la riattivazione dell'*account*, in quanto «l'esclusione dei ricorrenti da F. si pone in contrasto con il diritto al pluralismo di cui si è detto, eliminando o fortemente comprimendo la possibilità per l'Associazione ricorrente, attiva nel panorama politico italiano dal 2009, di esprimere i propri messaggi politici»[13].

Questo «approccio libertario»[14] è indubbiamente tanto attraente sul piano ideale,

---

7 Trib. Roma, sez. spec. imprese, ord. 12 dicembre 2019.

8 *Ibid.*

9 *Ibid.*

10 *Ibid.*

11 Sul tema della complessa relazione tra formazioni politiche e piattaforme si rinvia a G. Grasso, *Social network, partiti politici e lotta per il potere*, in questa *Rivista*, 1, 2020, 211 ss.

12 I. M. Lo Presti, *CasaPound, Forza Nuova e* Facebook. *Considerazioni a margine delle recenti ordinanze cautelari e questioni aperte circa la relazione tra partiti politici e* social network, cit., 927.

13 Trib. Roma, sez. spec. imprese, ord. 12 dicembre 2019.

14 Così C. Caruso, *I custodi di silicio. Protezione della democrazia e libertà di espressione nell'era dei social network*, in *Consulta Online*, 17 marzo 2020, 8.

quanto, a mio avviso, fragile sul piano sistematico.

Il riconoscimento da parte del giudice di effetti orizzontali dei diritti fondamentali, anche nei rapporti tra privati[15], tende a garantire a tutti uno spazio pubblico, un "*Hyde Park Corner* digitale" e richiama l'ideale originario di internet quale luogo ove si realizza compiutamente il mito del *free market of ideas*. E ciò appare in linea con l'impostazione della Costituzione italiana, che mostra una fede nel metodo della democrazia tale da consentire la partecipazione al dibattito pubblico anche ai "nemici della libertà", al dissenso più estremo, non richiedendo adesione ai valori democratici, ma "lealtà di comportamento" nella vita pubblica[16].

Inoltre, la prevalenza dell'indirizzo libertario costituirebbe un freno a quella tendenza, sempre più forte specie nell'ambito europeo, ad attribuire ai giganti del *web* il compito di "ripulire" la zona grigia della rete, rimuovendo dall'arena digitale quelle espressioni che sembrano pericolose, anche se non necessariamente illecite (a titolo di esempio, la disinformazione, i contenuti antiscientifici, i discorsi razzisti o discriminatori anche se non superano la soglia del penalmente illecito)[17].

Tale orientamento, sebbene suggestivo, suscita una serie di perplessità anche a livello teorico che spiegano forse anche il suo scarso seguito in giurisprudenza, almeno sino ad ora.

L'inquadramento delle piattaforme come "fori pubblici" o comunque soggetti esercenti un servizio pubblico appare problematico, trattandosi di imprese che perseguono finalità commerciali e che non hanno, *ex lege*, obblighi di servizio pubblico e di pluralismo interno[18]. L'ordinanza romana, infatti, sembra trarre da una situazione di mero fatto (l'indubbio rilievo delle piattaforme) conseguenze abnormi sul piano giuridico, quali l'obbligo di ospitare qualunque idea che non sia illecita. Come sottolinea con chiarezza Pietro Villaschi, una simile linea argomentativa sconta «un vizio di fondo, in quanto, in assenza, come si diceva, di una solida ricostruzione dottrinale e giurisprudenziale, va di fatto surrettiziamente a configurare come pubblici soggetti che tali non sono, né offrono un servizio pubblico (come, invece, per fare un esempio legato sempre al mondo dei media è un ente come la RAI). In altri termini, l'esito che si produce è quello di una confusione e di uno snaturamento circa lo status giuridico di tali entità, alle quali viene imposta l'osservanza di principi e obblighi che tradizionalmente

[15] Un esplicito richiamo alla teoria degli effetti orizzontali si rinviene anche in una recente ordinanza del Tribunale di Varese, sez. I, 2 agosto 2022, in un caso relativo alla rimozione di un video con l'intervento nell'aula parlamentare di un deputato anti-vax. Anche in questa vicenda il giudice ha ritenuto che l'autonomia privata possa essere limitata dall'ordinamento giuridico nella sua complessità e non possa comprimere un diritto costituzionale dell'utente, a meno che tale limitazione sia finalizzata alla tutela di un diritto di rilevanza costituzionale (nel caso in esame, la salute). In questo caso, però, l'esito è stato favorevole a Facebook. Tale decisione si può leggere in questa *Rivista*, 3, 2022, con una acuta nota di M. Gozzi, *Internet e "standard della community" nella regolamentazione delle piattaforme online: sulla non vessatorietà delle clausole in materia di disinformazione*, 308 ss.

[16] In questo senso, C. Caruso, *I custodi di silicio. Protezione della democrazia e libertà di espressione nell'era dei social network*, cit., 9. Per un approfondimento, rinvio a G.E. Vigevani, *Radici della Costituzione e repressione della negazione della Shoah*, in *Rivista Associazione Italiana dei Costituzionalisti*, 4, 2014, 14 ss.

[17] Si consenta ancora un richiamo a un mio recente lavoro, *Piattaforme digitali private, potere pubblico e libertà di espressione*, in *Diritto costituzionale*, 1, 2023, 41 ss.

[18] In questo senso S. Piva, *Facebook è un servizio pubblico? La controversia su CasaPound risolleva la quaestio dell'inquadramento giuridico dei social network*, cit., 1208.

il nostro ordinamento non riserva a soggetti privati, con ricadute in termini di tutela di altri valori e interessi costituzionalmente rilevanti»[19].
Porre per via giurisprudenziale o anche per via legislativa[20] un divieto per i *social media* di moderare i contenuti e di rimuovere *post* basati sull'ideologia politica, sia pure ritenuti odiosi o discriminatori, comprime inoltre il diritto della piattaforma a definire una qualche linea editoriale o, almeno, a non dare spazio a soggetti le cui opinioni confliggono con i valori della piattaforma stessa o possono danneggiare il proprio *business*.
Infine, resta la distinzione tra diritto di parola e diritto al mezzo, che non ha esplicito riconoscimento nella giurisprudenza costituzionale. Secondo la Corte, infatti, «che "tutti" abbiano diritto di manifestare il proprio pensiero "con ogni mezzo", non può significare che tutti debbano avere, in fatto, la materiale disponibilità di tutti i possibili mezzi di diffusione, ma vuol dire, più realisticamente, che a tutti la legge deve garantire la giuridica possibilità di usarne o di accedervi»[21]. Tale principio sembra doversi estendere anche alla rete e, in particolare, ai *social network*, nonostante l'evidente diversità rispetto agli strumenti di comunicazione precedenti, pena la trasformazione per via giurisprudenziale di un diritto di libertà delle piattaforme in una funzione legislativamente attribuita al solo servizio pubblico, quella di assicurare il "pluralismo interno".

3. L'approccio protezionistico: una piattaforma ha il dovere legale di rimuovere contenuti discriminatori di cui è a conoscenza, in ragione della sua speciale posizione e della attività di indubbio rilievo sociale che svolge

L'approccio opposto, ma sempre nel quadro di una concezione "pubblicistica" della funzione delle piattaforme digitali, postula non solo la facoltà ma in taluni casi persino l'obbligo in capo alle medesime di rimuovere contenuti discriminatori.
Anche tale orientamento ha avuto una applicazione piuttosto limitata. A quanto consta, è stato accolto in due pronunce sempre del Tribunale di Roma, la più risalente concernente un ricorso in via cautelare promosso da "Forza nuova"[22], la più recente a conclusione del procedimento di primo grado nella controversia promossa da "CasaPound" che, come si è detto, in sede cautelare aveva condotto alla provvisoria riattivazione dell'account del movimento della destra estrema italiana[23].

[19] P. Villaschi, *Facebook come la RAI?: note a margine dell'ordinanza del Tribunale di Roma del 12.12.2019 sul caso CasaPound c. Facebook*, cit., 441.

[20] A titolo di esempio, nel contesto statunitense si può richiamare la tanto discussa – e già oggetto di una complessa vicenda giudiziaria – legge texana conosciuta come «HB20», di stampo conservatore, la quale mira a vietare alle grandi piattaforme di *social media* di rimuovere, moderare o etichettare i messaggi dagli utenti in Texas in base a «*specific viewpoints*».

[21] Corte cost., 15 giugno 1972, n. 105; nello stesso senso A. Pace-M. Manetti, *Art. 21. La libertà di manifestazione del proprio pensiero,* in G. Branca (a cura di), *Commentario alla Costituzione*, Bologna-Roma, 2006, 361.

[22] Trib. Roma, sez. dir. della persona, ord. 23 febbraio 2020, confermata in sede di reclamo.

[23] Trib. Roma, sez. dir. della persona, sent. 5 dicembre 2022, n. 17909, che sembra allo stato chiudere il

Entrambe le pronunce concludono nel senso che la piattaforma non solo ha il diritto, ma anche il dovere di rimuovere contenuti discriminatori e di incitazione all'odio, di combattere la disinformazione, di tutelare la salute pubblica, in base al diritto sovrannazionale e anche agli impegni assunti con la Commissione europea e non solo alle *policies* del *social*[24]. E ciò anche a prescindere dalla illiceità sul piano penale di tali contenuti.

Le due pronunce – del tutto sovrapponibili, anche perché frutto della penna del medesimo Giudice – sono senza dubbio assai articolate.

Esse, in primo luogo, ricostruiscono i limiti alla libera manifestazione del pensiero in relazione ai messaggi di incitamento all'odio e alla discriminazione, in particolare alla luce del diritto internazionale, del diritto eurounitario, della normativa e della giurisprudenza Cedu nonché nelle iniziative dell'Unione volte a contrastare i discorsi d'odio, oltre che del diritto nazionale.

Alla luce del quadro normativo delineato, concludono nel senso che:

a) la libertà di manifestazione del pensiero non include discorsi ostili e discriminatori (vietati a vari livelli dall'ordinamento interno e sovranazionale);

b) gli obblighi derivanti dal diritto sovranazionale impongono di esercitare un controllo agli stati ed anche, entro certi limiti, ai *social network* come Facebook, che ha sottoscritto l'apposito Codice di condotta;

c) la chiusura di un *account* non determina una generalizzata compressione per via giudiziaria della libertà di espressione di singoli individui o gruppi, ma della possibilità di accedere ad uno specifico *social network* (che è anche un *social media*, strumento attraverso il quale i produttori di contenuti sono in grado di raggiungere il grande pubblico), gestito da privati, al fine di consentire la diffusione di informazioni concernenti l'attività di una determinata formazione politica;

d) non si può sottovalutare il ruolo spettante a Facebook in materia anche con riferimento al rischio della diffusione in forma "virale" di discorsi d'odio o di discriminazione[25].

Dopo una ricostruzione del quadro normativo in ottica multilivello, il Giudice non tralascia di ricordare che Facebook, soggetto privato che svolge un'attività economica, regola il rapporto tra i singoli utenti e tra questi ultimi e la piattaforma attraverso delle *policies*, ovvero le già richiamate condizioni contrattuali che l'utente deve accettare al momento dell'iscrizione alla piattaforma[26]. Tra queste "regole di comportamento", vi

lungo contenzioso tra CasaPound e Facebook (oggi Meta Platforms Ireland Ltd). In essa il giudice del merito ribalta l'esito del procedimento cautelare promosso da CasaPound e dal suo dirigente Davide Di Stefano nei confronti di Facebook, revocando l'ordinanza emessa in 12 dicembre 2019 e rigettando le domande risarcitorie.

[24] In particolare, in entrambe le pronunce si legge che si legge che: «I contenuti, che inizialmente erano stati rimossi e poi a fronte della reiterata violazione hanno comportato la disattivazione degli *account* […] sono illeciti da numerosi punti di vista. Facebook non solo poteva risolvere il contratto grazie alle clausole contrattuali accettate al momento della sua conclusione, ma aveva il dovere legale di rimuovere i contenuti, una volta venutone a conoscenza, rischiando altrimenti di incorrere in responsabilità […], dovere imposto anche dal codice di condotta sottoscritto con la Commissione Europea» (ord. 23 febbraio 2020, 43 e sent. 5 dicembre 2022, 39-40).

[25] Sent. 5 dicembre 2022, n. 17909, 23.

[26] Ivi, 23-26.

è anche quella di non usare Facebook per scopi discriminatori e, inoltre, viene specificato che su questo *social network* non è ammessa la presenza di organizzazioni o individui che proclamano missioni violente o che sono coinvolti in azioni violente. In caso di violazione degli standard richiamati, Facebook si considera legittimato ad assumere misure restrittive nei confronti dell'*account* in questione, senza tra l'altro essere tenuto ad un obbligo di preavviso.

Il Tribunale ritiene altresì che: «Le regole più stringenti in ordine alle legittimità dei contenuti divulgabili in rete sono determinate anche dall'effetto moltiplicatore di Internet, idoneo ad attribuire un'attitudine lesiva a condotte che altrimenti potrebbero non averne, da qui le iniziative volte a responsabilizzare i gestori dei *social network* onde vietare la diffusione di simboli o discorsi d'odio in rete anche attraverso le condizioni contrattuali che ogni utente deve sottoscrivere al momento dell'iscrizione»[27]. Con questo passaggio di grande significato, l'organo giudicante ammette la possibilità di prevedere per il "mondo" dell'*online* delle regole più ferree – e, di conseguenza, maggiormente limitative della libera manifestazione del pensiero – rispetto a quando il medesimo diritto viene esercitato *offline*.

Sulla base di queste considerazioni e dopo un esame dettagliato dei contenuti postati sulla pagina di Casapound[28] – e più in generale delle idee e delle azioni del movimento, anche al di fuori della piattaforma – il Giudice conclude che «le parti attrici hanno pubblicato contenuti in violazione delle clausole contrattuali che vietano il supporto ad organizzazioni d'odio (Davide Di Stefano attraverso il proprio profilo anche quale amministratore della pagina di CasaPound Italia), la pubblicazione di *hate speech* basati sulla razza o etnia (art 13 Standard della Comunità) e simboli che rappresentano/elogiano un'organizzazione che incita all'odio (come tutta la simbologia fascista o l'elogio ai combattenti della X Mas o della Repubblica di Salò- art 2 degli Standard) o che incitano alla violenza (art 1 degli Standard)»[29].

Anche questo approccio di natura protezionistica, volto a concepire le piattaforme come una sorta di "controllori della rete" (i quali non solo possono ma devono rimuovere certi contenuti in un'ottica di depurazione del dibattito pubblico *online*), suscita più di una perplessità.

Un primo aspetto su cui il Giudice sembra non esprimersi a sufficienza riguarda l'indicazione dei casi in cui la piattaforma sarebbe tenuta all'intervento restrittivo dell'*account* o del contenuto postato, in quanto si limita semplicemente a statuire che «Facebook non solo poteva risolvere il contratto grazie alle clausole contrattuali accettate al momento della sua conclusione, ma aveva il dovere legale di rimuovere i contenuti, una volta venutone a conoscenza, rischiando altrimenti di incorrere in responsabilità […]»[30].

L'interrogativo che sorge spontaneo è il seguente: quando si può ritenere che la piattaforma "è venuta a conoscenza" del contenuto poi da rimuovere? Deve, ad esempio, effettuare un controllo di tipo preventivo su tutti i contenuti prima di immetterli

[27] Ivi, 31.

[28] Ivi, 26-39.

[29] Ivi, 39.

[30] Ivi, 40.

in rete? Oppure deve attivarsi solo in presenza di una segnalazione, anche generica, proveniente da altri utenti che entrano in contatto con il contenuto dubbio? Oppure, ancora, la piattaforma è tenuta all'intervento limitativo solo in presenza di un provvedimento dell'autorità pubblica che glielo imponga?

Questo profilo è in realtà di estrema rilevanza in quanto a seconda delle risposte a tali interrogativi discendono diverse forme di responsabilità per la piattaforma: infatti, imporre ai *social network* controlli preventivi – obbligo che non si rinviene nella Direttiva *e-commerce*[31] e che non è previsto nemmeno nel più recente *Digital Services Act*[32] – è ben diverso dal prevedere forme di responsabilità solo qualora il *social network* non rimuova un contenuto che invece l'autorità pubblica gli ha ordinato, con un provvedimento motivato, di eliminare.

Inoltre, non va dimenticato che distinguere tra lecito e illecito non è affatto agevole[33], in quanto anche nella legislazione vigente i confini del concetto di "discorso d'odio" non sono di facile perimetrazione e variano da Stato a Stato nel contesto europeo. Ciò nonostante, questo aspetto viene invece quasi dato per scontato dal Giudice romano.

Il profilo problematico di questa ricostruzione mi pare dunque evidente: se si decide di consegnare, anche attraverso atti normativi, alle piattaforme digitali (soggetti privati) compiti di controllo sul discorso pubblico *online* – compiti che, tradizionalmente, spettano alle autorità pubbliche, le quali per esercitarli devono tuttavia rispettare le regole costituzionali poste a tutela di una effettiva libertà di parola – si deve accettare l'idea che le stesse divengano titolari di sempre maggiori poteri decisori, soprattutto per quanto concerne lo stabilire cosa si può e cosa invece non si può "dire" *online*. Ammettere che tali soggetti privati esercitino pressoché quotidianamente poteri di controllo sui contenuti postati in rete significa accrescere inevitabilmente il potere delle piattaforme, le quali potrebbero in questo senso divenire sempre più "pericolose". Chi, a quel punto, controllerà i controllori?

Alla luce di questo ragionamento, le obiezioni mi paiono davvero significative, perché tale concezione finisce con il delegare a soggetti privati l'*enforcement* delle politiche pubbliche, senza quei vincoli procedurali – intervento del giudice, contraddittorio, etc. – che caratterizzano gli ordinamenti costituzionali. Mi pare una concezione che riflette una tendenza culturale, specie con lo sviluppo dei *social*, a guardare al diritto alla manifestazione del pensiero con diffidenza: da colonna portante della democrazia a strumento per attaccare privati cittadini (specie se gruppi di minoranze) e per destabilizzare gli ordinamenti democratici[34]. E, collegata a questa, una certa crisi di fiducia

[31] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»).

[32] Regolamento UE 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

[33] In questo senso, sono a mio avviso del tutto condivisibili i dubbi di Ginevra Cerrina Feroni: «*Who has the authority to distinguish between good and evil, between what people can say and what they cannot say? Who can define ethically and legally valid boundaries of individual thought and actions? And, finally, on the basis of what parameters, criteria, procedures and controls can all this be done?*». Cfr. G. Cerrina Feroni-A. Gatti, *Online Hate Speech and the Role of Digital Platforms: What Are the Prospects for Freedom of Expression?*, cit., 262.

[34] Cfr. anche V. Zeno-Zencovich, *The EU regulation of speech. A critical view*, in questa *Rivista*, 1, 2023,

nel metodo democratico, nella convinzione che la democrazia sia più forte dei suoi nemici.

4. L'approccio privatistico: la piattaforma è gestita da una società privata e gli accordi contrattuali tra essa e suoi utenti sono espressione dell'autonomia privata

L'indirizzo sinora maggioritario[35], almeno alla luce delle mie ricerche, riconduce invece il rapporto tra i *social* e gli utenti a un rapporto privatistico di natura contrattuale e ridimensiona la portata della libertà di informazione (e del relativo pluralismo), che non può, secondo quest'ottica, essere concepito come il diritto di poter diffondere le proprie idee in ogni luogo e in ogni spazio.
Questo orientamento si differenzia dai due precedenti di impostazione pubblicistica in quanto si allontana dalla concezione delle piattaforme digitali come soggetti esercenti attività di interesse pubblico, sottolineando il loro carattere prettamente privatistico: difatti, nonostante la indubbia e incontestata diffusione e rilevanza sociale, le piattaforme digitali rimangono dei soggetti sostanzialmente non pubblici, il cui rapporto con gli utenti va ricondotto principalmente ad un contratto di diritto privato[36].
Sulla base di questa impostazione, la piattaforma potrà rimuovere i contenuti non ammessi dagli *standard* della *community*, nei quali, tra l'altro, la stessa può anche decidere di vietare delle manifestazioni del pensiero che in realtà, per il diritto positivo, non sono illecite o penalmente rilevanti, come già accennato.
Le misure volte alla rimozione di tali contenuti – o quelle limitative dei relativi *account* – sono state ricondotte sia dal Tribunale di Siena che da quello di Trieste (sempre in casi in materia di discorsi d'odio) al diritto di recesso per giusta causa esercitato da una delle due parti, la piattaforma, a fronte del non rispetto da parte dall'altro contraente, ovvero l'utente, delle condizioni contenute nel contratto tra di loro esistente[37].
Inoltre, il Tribunale di Milano – in un caso di una società editrice "bannata" da YouTube per contenuti no-vax – ha chiaramente affermato che non è ravvisabile, al di fuori del contratto, un obbligo in capo a Google di garantire agli utenti di esprimere

12 ss. Si pensi, inoltre, alla "vicenda Trump" in relazione alla questione del c.d. *deplatforming*. Per questo tema, si veda M. Bassini, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in questa *Rivista*, 2, 2021, 67 ss.

[35] Trib. Siena, sez. un. civ., ord. 19 gennaio 2020, in cui il tribunale è stato chiamato a pronunciarsi a seguito di un ricorso promosso da un attivista di CasaPound, che lamentava la cancellazione del suo profilo Facebook a causa della diffusione di messaggi ritenuti a contenuto pericoloso e diffamatorio; Trib. Trieste, sez. civ., ord. 27 novembre 2020; Trib. Varese, sez. I civ., ord. 2 agosto 2022; Trib. Milano, sent. 19 luglio 2021.

[36] A p. 4 dell'ordinanza del Tribunale di Siena appena citata si legge che «[…] né la società resistente può seriamente essere paragonata ad un soggetto pubblico nel fornire un servizio, pur di indubbia rilevanza sociale e socialmente diffuso, comunque prettamente privatistico».

[37] Ivi, 4-5: «Tanto premesso, la società resistente ha compiutamente motivato e documentato il proprio buon diritto, di origine contrattuale, a procedere alla disattivazione della pagina e del profilo del ricorrente. […] Nell'ambito di un accordo di diritto privato la scelta di privare l'utente della piattaforma social rientra nel diritto di recesso, peraltro compiutamente regolamentato».

pubblicamente le proprie opinioni attraverso i *social media* e questo anche perché, come evidenza altresì il Tribunale di Siena, all'utente rimane sempre la possibilità concreta di continuare a diffondere i propri contenuti attraverso altri strumenti. La giurisprudenza di merito sembra quindi confermare l'insussistenza di una sorta di "diritto al *post*", cioè a poter fruire di uno spazio *online* o di un mezzo per potersi esprimere, in quanto la piattaforma digitale rimane un soggetto privato che può stabilire liberamente sulla base di quali regole gestire la propria attività economica, escludendo dalla stessa i soggetti che non le rispettano.

Tale libertà riconosciuta alle piattaforme non deve, tuttavia, trasformarsi in una forma di arbitrio: in questo modo, si permetterebbe alle piattaforme *social* di esercitare un potere davvero rilevante – ovvero quello di stabilire cosa può e cosa non può essere pubblicato in rete – senza limitazione alcuna[38].

Difatti, riconosciuta a Facebook la facoltà di stabilire discrezionalmente le proprie condizioni contrattuali, bisogna tuttavia accertare che il rapporto che viene a crearsi sia tendenzialmente equilibrato tra i due contraenti[39]. In verità, non si può non riconoscere che il contratto di cui si discute costituisce un rapporto tale per cui uno dei due contraenti, il più "forte" (anche da un punto di vista economico), detta le regole (che poi applica e sulla base delle quali assume decisioni) unilateralmente, con la conseguenza di "relegare" inevitabilmente la controparte (cioè l'utente) ad una condizione di "inferiorità" decisionale: l'alternativa che si presenta all'utente è accettare o non accettare queste condizioni, senza poterle negoziare. È chiaro, dunque, che se si volesse far prevalere una impostazione di questo tipo, bisognerebbe evitare di lasciare l'utente "in balìa" delle decisioni totalmente discrezionali dei colossi del *web*, auspicando la predisposizione, anche a livello normativo, di un minimo di garanzie a tutela della parte più "debole" di questo rapporto contrattuale.

Fatta questa precisazione, le ragioni per le quali questa impostazione mi sembra, tra quelle presentate, la più convincente sono varie. Innanzitutto, non comporta una delega di funzioni pubbliche a soggetti privati, né uno snaturamento della natura giuridica dei *social* che ancora mi pare non possano essere considerati un vero e proprio servizio pubblico; in aggiunta, vi è forse un minor rischio di una sorta di "*patchwork*" giurisprudenziale nel quale la sensibilità del giudicante rischia di divenire il dato decisivo; infine, la stessa mantiene la distinzione tra diritto di manifestazione del pensiero, che deve essere garantito a tutti e non ostacolato, e diritto al mezzo, che, invece, ancora non può ritenersi sussistente, come già accennato.

---

[38] Si veda M. Gozzi, *Internet e "standard della community" nella regolamentazione delle piattaforme online: sulla non vessatorietà delle clausole in materia di disinformazione*, cit., 312, dove l'autore afferma: «E sotto tale profilo, appare corretta l'affermazione svolta nel provvedimento annotato secondo la quale l'autonomia privata esercitata nell'elaborazione di norme di comportamento alle quali gli utenti aderiscono non è illimitata, né insindacabile, essendo soggetta, oltreché al rispetto delle norme imperative, *ex* art. 1418 c.c., ai limiti che la legge impone alla autonomia contrattuale».

[39] Su questo aspetto si sofferma la già richiamata ordinanza del Tribunale di Varese a p. 13: nel caso di specie, il giudice esclude l'eccepito carattere vessatorio delle clausole contrattuali che attribuiscono a Facebook il diritto unilaterale di sospendere a suo insindacabile giudizio l'*account* dell'utente ma, nonostante ciò, cerca di verificare se nel caso concreto «le condizioni d'uso alle quali la ricorrente ha aderito determinano a carico della stessa, quale consumatore, uno squilibrio dei diritti e degli obblighi contenuti nel contratto».

Resta, tuttavia, un tema di fondo, ovvero quello dei limiti al potere delle piattaforme di influire sul discorso pubblico, il quale si collega alla questione della qualificazione giuridica delle piattaforme. Nonostante, infatti, le piattaforme siano dei soggetti sostanzialmente privati, è innegabile che le stesse costituiscono dei veri e propri poteri che si affiancano a quelli più tradizionali[40]. E in questo senso, è certamente vero che «le maggiori piattaforme svolgono un ruolo di *gatekeeper* anche nel campo delle libertà di espressione e di informazione, atteso che le piattaforme incidono direttamente sulla diffusione delle notizie e in generale delle idee»[41].

Quali conseguenze, tuttavia, discendono dalla qualificazione delle piattaforme come "poteri privati"?

Secondo l'opinione di Ottavio Grandinetti e di altri giuristi, l'attività delle piattaforme sarebbe da ricollegare alla libertà di iniziativa economica privata, disciplinata in Costituzione all'art. 41, con la conseguenza logica di ammettere limitazioni alla stessa al fine di salvaguardare valori come sicurezza, libertà e dignità umana oltreché in ogni caso di contrasto dell'attività con l'utilità sociale[42].

Al contrario, ritengo invece che, considerati gli ampi confini dell'art. 21, le attività economiche che hanno, tra gli altri, anche il compito di veicolare di informazioni dovrebbero rientrare, almeno rispetto a questa funzione, nell'ambito di tutela della norma costituzionale appena citata. In sostanza, il dato di fatto che la piattaforma digitale abbia una finalità lucrativa non preclude la possibilità che l'attività della stessa rientri nell'ambito di applicazione dell'art. 21, il che comporta la conseguenza di ammettere limiti in casi più circoscritti rispetto a quelli contemplati nell'art. 41.

5. Conclusioni: alcune strategie ragionando a partire dai principi fondanti il costituzionalismo classico

L'analisi giurisprudenziale appena conclusa dimostra l'eterogeneità delle posizioni assunte dai giudici italiani riguardo questi temi molto attuali. Le vicende giudiziarie riguardanti gli *account social* di movimenti politici come Casapound e Forza Nuova hanno visto l'instaurarsi di un vero e proprio dibattito tra commentatori, che hanno ragionato sulle relative pronunce, conferendo loro notevole rilievo. Tuttavia, mi sembra che sinora la giurisprudenza maggioritaria si stia assestando attorno all'ultima di queste impostazioni, relegando tali pronunce ad essere dei casi isolati: mi pare, infatti, che l'approccio più accolto sia anche il più logico e, al contempo, il più aderente al sistema costituzionale.

In questo quadro, restano tuttavia aperti alcuni interrogativi accennati in apertura di questo scritto. E dunque è doveroso provare a prospettare alcune possibili strategie, alla luce dei principi del costituzionalismo classico e anche della normativa europea *in fieri*. Strategie che mirano, da un lato, ad evitare che, le uniche "risposte" vengano

[40] Sul tema, sia consentito rinviare a G.E. Vigevani, *Informazione e potere*, in *Potere e Costituzione*, *Enciclopedia del Diritto, I tematici*, M. Cartabia-M. Ruotolo (diretto da), vol. 5, Milano, 2023, 219 ss.

[41] O. Grandinetti, *Le piattaforme digitali come "poteri privati" e la censura online*, cit., 179.

[42] Ivi, 180.

fornite dal formante giurisprudenziale ma anche, d'altro lato, a porre un freno al già consistente potere di cui godono le principali piattaforme digitali.

Anzitutto, in luogo di imporre alle piattaforme obblighi di pluralismo interno (che, almeno allo stato attuale, gravano solamente in capo al servizio pubblico), sarebbe invece auspicabile rivalutare il principio del pluralismo esterno, in modo da favorire la creazione di un sistema digitale plurale e competitivo. Mi sembra che questa sia la direzione nella quale anche il legislatore europeo, seppur prudentemente, abbia deciso di muoversi con l'adozione del c.d. *Digital Markets Act*[43]. Quest'ultimo prevede una disciplina *ad hoc* per i mercati digitali e ha come primario scopo quello di assicurare che quelli in cui agiscono i c.d. *gatekeepers*[44] siano equi e contendibili, cercando di "smantellare" le alte barriere all'ingresso in modo da renderli maggiormente concorrenziali e distribuendo così in modo più equilibrato il potere nel settore del digitale. La volontà del legislatore europeo pare essere quella di evitare che il potere rimanga nelle "mani" di pochi attori privati e, quindi, di scongiurare la persistenza di oligopoli – o addirittura monopoli – in questi ambiti rilevanti, regolando le posizioni dominanti anche con misure *ex ante*[45].

Vi è poi un ulteriore tema rilevante che coinvolge il principio di trasparenza, un valore dalle plurime declinazioni su cui anche il *Digital Services Act* sembra investire.

Da un lato, sembra necessario – anche se non del tutto agevole – garantire maggiore trasparenza dell'algoritmo che costituisce la base del funzionamento dei *social network* e dei motori di ricerca, il quale viene molto spesso custodito "gelosamente" dalle piattaforme stesse. Ciò implica innanzitutto cercare di rendere "pubblica" perlomeno quella parte dell'algoritmo che permette di comprendere i criteri decisionali adottati dalle piattaforme, ma comporta anche, in secondo luogo, la necessità di verificare l'eventuale interferenza statale nella definizione dello stesso, la quale potrebbe orientare o, addirittura, "inquinare" il libero mercato delle idee.

D'altro lato, vi è poi un ulteriore ricetta in materia di trasparenza che si collega a un principio del costituzionalismo, ovvero quello che concerne la trasparenza circa la provenienza dei contenuti. Infatti, i c. 3 e 5 dell'art. 21 della Costituzione sottolineano l'importanza della responsabilità personale di chi divulga informazioni e idee: nella Carta costituzionale, infatti, la riconosciuta libertà in materia di manifestazione delle idee non può essere scissa dalla responsabilità di chi esercita questo diritto, in quanto il

[43] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali).

[44] Art. 3, par. 1, regolamento (UE) 2022/1925: «Un'impresa è designata come *gatekeeper* se: a) ha un impatto significativo sul mercato interno; b) fornisce un servizio di piattaforma di base che costituisce un punto di accesso (*gateway*) importante affinché gli utenti commerciali raggiungano gli utenti finali; e c) detiene una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisisca siffatta posizione nel prossimo futuro».

[45] Per un commento a questo atto normativo si veda F. Zorzi Giustiniani, *L'Unione europea e regolamentazione del digitale: il Digital Services Package e il Codice di buone pratiche sulla disinformazione*, in *Nomos. Le attualità del diritto*, 2, 2022; P. Dunn, *Il Digital Markets Act: tra logiche concorrenziali e istanze costituzionali*, in *Diritti comparati*, 17 febbraio 2022; C. Hassan-C. Pinelli, *Disinformazione e democrazia. Populismo, rete e regolazione*, Venezia, 2022, 136-140. Per una analisi più ad ampio spettro degli approcci *antitrust* nell'ambito delle piattaforme *online* si veda O. Grandinetti, *Le piattaforme digitali come "poteri privati" e la censura online*, cit., 176-179.

pensiero espresso deve sempre essere riconducibile ad un soggetto specifico. Muovendosi da questo "dato" costituzionale, si potrebbe pensare di imporre alle piattaforme di accertare e indicare chi posta il contenuto (ad esempio, segnalando se si tratta di una persona fisica, una persona giuridica, un organo governativo, un programma automatico come un *bot* oppure un utente anonimo[46]) e da quale parte del mondo provenga, permettendo così agli altri utenti del *web* di valutare più consapevolmente l'informazione che incontrano nel *cyberspazio*[47].

Guardando oltreoceano, sembrano muoversi in questa direzione alcune normative nel contesto statunitense: ad esempio, nello Stato della California dal 1° luglio 2019 vige l'obbligo per le piattaforme digitali di etichettare i *bots* in modo da renderli facilmente riconoscibili agli utenti[48].

Inoltre, sempre sulla scia del dettato costituzionale (art. 21, c. 4) si potrebbe richiedere ai *social network* di indicare le fonti di finanziamento di coloro che veicolano informazioni, in modo da svelare quali soggetti – e, in senso più ampio, quali poteri – si celano dietro talune notizie divulgate *online*.

Infine, sarebbe indispensabile prevedere una serie di garanzie a tutela del soggetto fruitore della piattaforma, le quali dovrebbero tradursi in maggiore tassatività e determinatezza delle condizioni contrattuali, delle procedure di verifica interne e delle sanzioni applicabili[49]: definire chiaramente e rendere noti i casi di rimozione dei con-

[46] Ad esempio, *bot* e utenti anonimi vengono spesso impiegati per veicolare disinformazione, anche quella "creata" attraverso le più recenti tecniche di Intelligenza Artificiale. Questi temi sono affrontati da ultimo in un interessante saggio di M. Cazzaniga, *Una nuova tecnica (anche) per veicolare disinformazione: le risposte europee ai deepfakes*, in questa *Rivista*, 1, 2023, 170 ss.

[47] Nella ricerca di una qualche ricetta che consenta di rimanere nei confini tracciati dalla Costituzione, meritano di essere riportate le parole di un maestro del giornalismo italiano, Ferruccio De Bortoli: «Allora vi chiederete quali possono essere i rimedi? Innanzitutto, la già richiamata salvaguardia del pluralismo delle voci, l'autorevolezza, la serietà e la responsabilità della professione giornalistica. Nell'era dell'intelligenza artificiale […] c'è anche un nuovo tema di regole e della loro esigibilità per il quale dovremmo sentirci tutti più impegnati. Per esempio la trasparenza degli algoritmi pur nel rispetto del segreto industriale. L'assoggettazione dei *social network* a un loro giudice naturale al quale il cittadino possa appellarsi. Le piattaforme dovrebbero poi sentirsi in obbligo di non ospitare più contenuti provenienti da robot o da *account* non accertati. O almeno di denunciarne la provenienza, in modo da mettere in guardia i lori iscritti. Questo non significa far venir meno la libertà di anonimato o di celarsi dietro un *nickname*, ma di consentirne l'eventuale individuazione nel caso di reati o di comunicazioni false e strumentali. Ma per perseguire questi obiettivi, dobbiamo essere coscienti di quanto pericolosa sia la trappola della censura educativa e di quanto elevato sia il rischio di esserne di fatto complici. Sprovveduti ma non innocenti»; F. De Bortoli, *Ordine, 60 anni. La trappola della censura educativa*, in questa *Rivista*, 3, 2022, 12-13.

[48] California State Senate, Bill no. 1001, chapter 892, 2018 (c.d. *Bolstering online transparency act*), disponibile sul sito *ca.gov*.

[49] In questo senso, mi appaiono particolarmente sagge le considerazioni di Paolo Zicchittu, quando sostiene che: «Una volta ponderati accuratamente tutti gli interessi coinvolti, una risposta più convincente per risolvere la questione, armonizzando così anche le necessità provenienti dai diversi sistemi di tutela e riavvicinando le diverse concezioni della democrazia, potrebbe essere, allora, quella di procedimentalizzare l'iter, che conduce all'oscuramento di una pagina social. La predeterminazione di una procedura certa, chiara e trasparente salvaguarderebbe i diritti dei singoli e delle associazioni, che subiscono la rimozione improvvisa del proprio profilo e ridurrebbe altresì l'attivismo dei giudici, conducendo a soluzioni tendenzialmente più univoche. Da questo punto di vista, Facebook dovrebbe, in primo luogo, assolvere a tutta una serie di obblighi informativi nei confronti degli utenti, con riguardo precipuo ai contenuti potenzialmente vietati. Secondariamente, occorrerebbe pure garantire ai soggetti sanzionati con l'oscuramento della pagina una sorta di diritto di difesa, assicurando loro

tenuti e di sospensione degli *account* e le relative procedure permette di garantire più certezza all'utente.

Mi si consenta, in chiusura, di porre un dubbio di carattere generale: sussiste davvero, come si sostiene generalmente, una contrapposizione tra un modello americano ispirato al *free speech* e un modello europeo attento alla tutela della dignità della persona e degli altri diritti individuali o semmai esistono una pluralità di modelli europei, che partono da una concezione non identica della democrazia ("protetta o "aperta") e si riflettono sui limiti dell'intervento pubblico sulla libertà di espressione?

Certo, decisioni come quelle oggetto di queste pagine, provvisorie ed eterogenee nel percorso argomentativo e nell'esito, non consentono di offrire risposte a un interrogativo così ampio e complesso. Esse, però, evidenziano una qualche distanza tra l'interpretazione prevalente dei confini della libertà di espressione nella giurisprudenza italiana e nelle corti europee. Mostrano, altresì, la difficoltà di una osmosi tra la tradizione costituzionale italiana e la sempre più forte spinta proveniente dalle istituzioni e dai giudici sovranazionali a limitare i discorsi d'odio.

il contraddittorio con gli amministratori della piattaforma, per illustrare le proprie ragioni». Cfr. P. Zicchittu, *I movimenti "antisistema" nell'agorà digitale: alcune tendenze recenti*, cit., 9.

Le Conclusioni dell'Avvocato Generale nel rinvio pregiudiziale C-178/22 promosso dal Tribunale di Bolzano: *quo vadis, data retention*?*

Giulia Formici

Abstract

Le recenti Conclusioni dell'Avvocato Generale Collins relative alla domanda di pronuncia pregiudiziale proposta dal Tribunale di Bolzano rappresentano l'occasione per tornare a riflettere sulla complessa e articolata disciplina della conservazione e accesso ai metadati per scopi securitari nell'UE e nel contesto italiano. Il presente contributo intende fornire alcune prime considerazioni critiche sul presente e sul futuro della *data retention* nonché sulle sfide che diversi attori, tanto a livello nazionale quanto sovranazionale, dovranno affrontare nel difficile bilanciamento tra sicurezza e tutela dei diritti fondamentali nell'era digitale.

The recent Opinion of the Advocate General related to the request for a preliminary ruling proposed by the Bolzano Tribunal represents a renewed opportunity to discuss about the complex and articulated discipline concerning the retention and access to metadata for security purposes. The paper aims at providing some initial evaluations on the state of the art as well as on the possible future developments on data retention regulation, both at national and supranational level: different actors – legislators and courts – should confront with the difficult challenge of balancing security needs and fundamental rights protection in the digital era.

Sommario

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

Generale Collins nel caso C-178/22. – 4. Tante tappe ma quale meta? La difficoltà di scorgere un punto di arrivo.

Keywords
data retention; rinvio pregiudiziale C-178/22; accesso ai metadati; sicurezza; diritti fondamentali

1. Il tortuoso percorso della *data retention* nell'Unione europea tra rallentamenti e inversioni di marcia

Le Conclusioni dell'Avvocato Generale nel caso C-178/22, avviato mediante rinvio pregiudiziale dal Tribunale di Bolzano[1], rappresentano solo l'ultima tappa della c.d. *data retention saga*. La disciplina della conservazione e accesso ai metadati per scopi securitari ha infatti seguito un percorso regolatorio, tra i più lunghi e travagliati nel contesto eurounitario, caratterizzato da molteplici battute d'arresto e inversioni di marcia nonché dal proliferare di sentieri normativi e giurisprudenziali paralleli, in cui legislatori e corti nazionali si sono spesso avventurati.
In questo articolato contesto, la Corte di giustizia dell'UE (CGUE) ha sicuramente contribuito, molto più di altri "viaggiatori", a dettare il passo e la direzione del cammino, a partire dalla prima pronuncia *Digital Rights Ireland*[2] sino ad arrivare, attraverso decisioni di estremo rilievo[3], alle recenti e fondamentali sentenze *Privacy International* e *La Quadrature du Net*[4] del 2020. Queste ultime[5] hanno innanzitutto rafforzato i principi già

[1] Conclusioni dell'Avvocato Generale Anthony Michael Collins, CGUE, C-178/22, sulla base della domanda di pronuncia pregiudiziale proposta dal Tribunale di Bolzano.

[2] CGUE, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications et al* (2014). Tra i numerosi commenti a questa storica pronuncia, si rinvia a: M. Dicosola, *La data retention directive e il dialogo tra Corti costituzionali e Corte di Giustizia nel sistema multilivello europeo*, in *Diritti comparati*, 20 febbraio 2014; M. Granger - K. Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection*, in *European Law Review*, 6, 2014, 849 ss; A. Vedaschi, *Data retention and its implications for the fundamental right to privacy*, in *Tilburg Law Review*, 20, 2015, 19 ss.; G. Caggiano, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in questa *Rivista*, 2, 2018, 64 ss.

[3] Si fa riferimento alle sentenze CGUE, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB e Secretary of State c. Post-och telestryrelsen (PTS) e Tom Watson et al.* (2016) e CGUE, C-207/16, *Ministerio Fiscal* (2018). Per un'analisi di tali pronunce sia consentito rinviare a G. Formici, *La disciplina della data retention tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, Torino, 2021 e alla bibliografia ivi citata.

[4] CGUE, C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs et al.* (2020) e CGUE, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net et al. v. Premier Ministre et al.* (2020). *Ex multis*, si rimanda, per un commento a: M. Rojszczak, *National security and retention of telecommunications data in light of recent case law of the European Courts*, in *European Constitutional Law Review*, 4, 2021, 607 ss.; V. Mitsilegas - E. Guild - E. Kuskonmaz - N. Vavoula, *Data retention and the future of large-scale surveillance: the evolution and contestation of judicial benchmarks*, in *European Law Journal*, 1, 2022, 1 ss.; S. Eskens, *The ever-growing complexity of the data retention discussion in the EU: an in-depth review of La Quadrature du Net & Others and Privacy International*, in *European Data Protection Law Review*, 8, 2022, 143 ss.; M. Tzanou - S. Karyda, *Privacy International and La Quadrature du Net: one step forward, two steps back in the data retention saga?*, in *European Public Law*, 1, 2022, 123 ss.; N. Ni Loideain, *EU data privacy law and serious crime. Data retention and policymaking*, Oxford, 2022.

[5] Merita ricordare sin da ora come le rilevanti pronunce del 2020 siano state seguite da alcune ulteriori sentenze della CGUE in materia di *data retention* che hanno rappresentato una conferma ulteriore

sanciti nella previa giurisprudenza europea[6]: da un lato viene ribadita l'incompatibilità con il diritto dell'UE di forme di conservazione generalizzata e indiscriminata (c.d. *bulk data retention*) per scopi di garanzia della sicurezza pubblica e repressione dei reati gravi, mentre dall'altro la *targeted data retention* viene riconfermata come l'unica forma di conservazione proporzionata e legittima. Sotto il profilo dell'accesso ai metadati da parte di autorità di *law enforcement* e di *intelligence*, inoltre, vengono riaffermati quali prerequisiti necessari tanto il carattere di gravità del reato perseguito, quanto il previo controllo da parte di un'autorità amministrativa indipendente o giurisdizionale connotata da indipendenza e terzietà. Accanto a tali importanti conferme, la CGUE non ha poi mancato di introdurre nelle due pronunce richiamate rilevanti novità, soprattutto per quanto concerne il vaglio di proporzionalità: per la prima volta viene promossa una significativa distinzione tra obiettivi di sicurezza pubblica e quelli di sicurezza nazionale[7], riconoscendo la maggiore rilevanza dell'ultima e quindi la possibilità di disporre, per tale finalità solamente, misure più invasive della sfera privata

dei principi e requisiti sanciti dai giudici di Lussemburgo: in particolare, si fa riferimento a CGUE, C-746/18, *HK v. Prokuratuur* (2021); CGUE, C-140/20, *GD v. Commissioner of An Garda Siochana et al.* (2022), e CGUE, cause riunite C-793/19 e C-794/19, *Bundesrepulik Deutschland v. SpaceNet AG e Telekom Deutschaland GmbH* (2022). Per uno studio di tali più recenti sentenze, si vedano, tra gli altri, S. Rovelli, *Case Prokuratuur: proportionality and the independence of authorities in data retention*, in *European Papers*, 2021, p. 199 ss.; E. Celeste, *Commission v. Spain and H. K. v. Prokuratuur: Taking the Plank out of EU's Own Eye*, in *BridgeBlog*, 15 marzo 2021; E. Andolina, *Ancora una pronuncia della Grande Camera della CGUE in tema di condizioni di accesso ai traffic data*, in *Processo Penale e Giustizia*, 5, 2021, 1195 ss.; X. Tracol, *The joined cases of Dwyer, SpaceNet before the European Court of Justice: the judgments of the Grand Chamber about data retention continue falling on deaf ears in Member States*, in *Computer Law & Security Review*, 48, 2023, 1 ss.; sia consentito anche il rinvio a G. Formici, *La CGUE torna a parlare agli Stati membri in materia di conservazione dei metadati e tutela dei diritti fondamentali: in un dialogo fra sordi, repetita iuvant?* , in *Diritti comparati*, 8 maggio 2023. In estrema sintesi, ciò che viene ribadito anche in tali ultime pronunce, è che «l'utilità della *data retention* per le investigazioni penali è indubbia; il modello di conservazione generalizzata e indifferenziata dei dati è inaccettabile in una società democratica; modelli alternativi di conservazione differenziata sono possibili e comunque spetta agli Stati l'obbligo di soluzioni ingegnose ma rispettose dei diritti sul punto; le eventuali difficoltà pratiche nel concepire detti modelli alternativi non possono costituire un pretesto per sposare o non abbandonare il modello generalizzato», R. Flor, S. Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale*, Torino, 2022, 31.

[6] Primo fra tutti il fatto che la disciplina della *data retention* rientra nell'ambito di applicazione della Direttiva *e-Privacy* (direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, direttiva relativa alla vita privata e alle comunicazioni elettroniche, c.d. Direttiva *e-Privacy,* GU 2002 L. 201/37) ogniqualvolta vengano sanciti obblighi in capo a *service providers* privati. Su questo dibattuto e tutt'altro che pacifico profilo, M. Zalnieriute, *A struggle for competence: national security, surveillance and the scope of EU la wat the Court of Justice of the EU*, in *Modern Law Review*, 85, 2021, 1 ss.

[7] La definizione di sicurezza nonché la linea di demarcazione – invero ricorrente e cruciale sotto il profilo del riparto di competenze tra UE e Stati membri – tra sicurezza nazionale e pubblica, resta un tema di estremo rilievo e complessità. Per riflessioni su tale concetto, si rinvia, *ex multis*, a P. Torretta, *Diritto alla sicurezza e (altri) diritti e libertà della persona: un complesso bilanciamento costituzionale*, in A. D'Aloia (a cura di), *Diritti e Costituzione. Profili evolutivi e dimensioni inedite*, Milano, 2003, 451 ss.; G. de Vergottini, *Guerra e Costituzione. Nuovi conflitti e sfide alla democrazia*, Bologna, 2004; T.E. Frosini, *Il diritto costituzionale alla sicurezza*, in *Forum di Quaderni Costituzionali*, 2006, 1 ss.; A. Vedaschi, *À la guerre comme à la guerre? La guerra nel diritto pubblico comparato*, Torino, 2007; T. Giupponi, *La sicurezza e le sue "dimensioni" costituzionali*, in S. Vida (a cura di), *Diritti umani. Teorie, analisi, applicazioni*, Bologna, 2008, 275 ss.; G. Cerrina Feroni - G. Morbidelli, *La sicurezza: un valore super primario*, in *Percorsi costituzionali*, 1, 2008, 31 ss.; ma anche, sotto il profilo del diritto eurounitario, P. Vogiatzoglou - S. Fantin, *National and public security within and beyond the Police Directive*, in A. Vedder - J. Schroers - C. Ducuing - P. Valcke (eds.), *Security and law. Legal and ethical aspects of public security, cyber security and critical infrastructure security*, Bruxelles, 2019, 27 ss.; M. Zalnieriute, *A struggle for competence: national security, surveillance and the scope of EU la wat the Court of Justice of the EU*, cit.

quali la *bulk data retention*, sebbene a specifiche condizioni e limiti[8].
Le articolate pronunce del 2020, i principi e limiti in esse sancite[9] hanno quindi certamente concorso a determinare «*an important barrier to the advent of a mass surveillance society*»[10], ponendosi in continuità e coerenza con una interpretazione "costituzionale" della disciplina della *data retention* che va ad inserirsi nella più ampia dinamica di «ridefinizione di un perimetro costituzionalmente orientato o quanto meno *human rights oriented* di disposizioni già in vigore quando la transizione da un'Europa dei mercati a un'Europa dei diritti non si era ancora del tutto completata»[11]. Nel fare questo, la CGUE non ha però mancato di adottare un approccio anche pragmatico – pur non scevro da critiche[12] – che ha ridefinito i contorni del vaglio di proporzionalità

[8] Questi limiti e condizioni possono essere così schematizzati: «il carattere non sistematico della conservazione generalizzata, la presenza di circostanze sufficientemente concrete che consentano di ritenere esistente una minaccia grave per la sicurezza nazionale reale e attuale o prevedibile, la previsione di un tempo di *data retention* limitato allo stretto necessario, la determinazione di garanzie rigorose contro il rischio di abusi, nonché la previsione di un effettivo controllo giurisdizionale o di un organo indipendente», G. Formici, *La sentenza HK c. Prokuratuur e il difficile dialogo tra CGUE e Stati membri in materia di conservazione e accesso ai metadati per finalità securitarie: spunti di riflessione su una questione vecchia ma ancora irrisolta*, in *Quaderni SIDIBlog*, 1, 2021, 237.

[9] La giurisprudenza della CGUE trova riflesso anche nelle decisioni di talune corti nazionali, come si avrà modo di approfondire anche nel prosieguo del presente lavoro. Per un'analisi dell'apporto del continuo dialogo tra corti nazionali e CGUE, si veda J. Podkowik - R. Rybski - M. Zubik, *Judicial dialogue on data retention laws: a breakthrough for European Constitutional Courts*, in *ICON-S*, 5, 2021, 1597 ss.

[10] V. Mitsilegas et al., *Data retention and the future of large-scale surveillance*, cit., 12; nello stesso contributo viene evidenziato come «*The evolution of the Court's case-law highlights the intricate institutional architecture at play when it comes to defining the future of mass surveillance and democracy in the digital era, with a complex part played by the judiciary, the legislative and the executive in a multi-level polity such as the EU*». Del resto, anche Fennelly riconosce il ruolo para-legislativo della CGUE, centrale nel percorso di "costituzionalizzazione" di taluni principi e requisiti in materia di sorveglianza massiva: «*the Court of Justice is arguably engaging in an exercise which would appear more legislative than judicial in its character (..). The Court in effect constitutionalizes these detailed requirements*», D. Fennelly, *Data retention: the life, death and afterlife of a directive*, in *ERA Paper*, 2018, 17; in questo senso, sul percorso di "costituzionalizzazione" della sorveglianza massiva operato dai giudici di Lussemburgo, sia consentito rinviare a E. Celeste - G. Formici, *Constitutionalizing mass surveillance in the EU: civil society demands, judicial activism and legislative inertia*, in *German Law Journal*, in corso di pubblicazione; ma si veda anche F-G. Wilman, *Two emerging principles of EU Internet Law: a comparative analysis of the prohibitions of general data retention and general monitoring obligations*, in *Computer Law & Security Review,* 46, 2022, 1 ss., che considera il divieto di *bulk data retention* come un principio generale della *EU Internet Law*; similmente anche M. Brkan, *Privacy, data protection and the role of European Courts: towards judicialization and constitutionalisation of European privacy and data protection framework*, in G. Gonzalez - R. Van Brakel - P. De Hert (eds.), *Research handbook on privacy and data protection law*, Londra, 2022, 274 ss.

[11] O. Pollicino - M. Bassini, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto penale contemporaneo*, 9 gennaio 2017.

[12] In senso critico M. Tzanou - S. Karyda, *Privacy International and La Quadrature du Net*, cit., che ravvisano nelle più recenti pronunce della CGUE e nel vaglio di proporzionalità ivi promosso, nella parte in cui viene riconosciuta la legittimità della *bulk data retention* per finalità di sicurezza nazionale, un passo indietro rispetto alle tutele previamente affermate. Problematicità, infatti, vengono riscontrate nella distinzione tra scopi di tutela della sicurezza nazionale e di quella pubblica, così come nella determinazione dei diversi limiti affermati dai giudici di Lussemburgo. Sebbene insomma alcuni autori abbiano riscontrato nelle pronunce *Privacy International* e *La Quadrature du Net* «*a culmination of efforts on behalf of the Court to reach a compromise and re-strike the balance between fundamental rights and the (loud and clear) desire of the Member States to uphold data retention schemes in favour of the latter*», essi non hanno mancato di rilevare come «*a clear distinction between the classification of the different public interest objectives may not always be an easy task. In any case, support for such reading does not seem to be widespread, as the judgments have not been received with enthusiasm by the Member States. On the contrary, Member States continue to try to find loopholes to circumvent the Court's findings, even though on initial observation, national courts seem to have followed them. The judicial acceptance of*

dinnanzi alle innegabili problematicità attuative e alle esigenze di garanzia della sicurezza nazionale evidenziate con forza negli anni dagli Stati membri.
Proprio per questa duplicità di profili, tensioni e soluzioni interpretative – che del resto riflettono la già nota difficoltà di attuare i principi di proporzionalità e necessità dinnanzi alle contrapposte spinte securitaria e garantista[13] –, le sentenze *Privacy International* e *La Quadrature du Net* hanno finito col ravvivare il mai sopito dibattito tra i diversi protagonisti del difficile percorso regolatorio della *data retention*.
Per parte della società civile e delle organizzazioni non governative (ONG) attive nell'ambito della tutela dei diritti alla privacy e alla protezione dei dati, la posizione espressa dalla CGUE costituisce il frutto di un mutato approccio più marcatamente pro-securitario, che finirebbe con il comprimere verso il basso le più garantiste tutele determinate nella previa *case law*[14].
Di segno opposto sono invece le perplessità evidenziate da numerosi Stati membri che hanno criticato la rigidità del vaglio di proporzionalità promosso: i limiti e le condizioni sancite condizionerebbero e limiterebbero eccessivamente la possibilità di impiego dei metadati, soprattutto quando ciò sia volto a scopi di lotta alla criminalità. Governi e legislatori nazionali, del resto, hanno sempre mostrato – e ancora mostrano, pur con diversi livelli di intensità – una certa resistenza nel modificare le normative interne in materia di conservazione e accesso ai metadati in senso conforme alla giurisprudenza della CGUE; le riforme che si sono avvicendate in molti Stati membri, pur disponendo salvaguardie più significative e profonde rispetto alle legislazioni dei primi anni 2000, non hanno infatti mai del tutto abbandonato l'imposizione di un obbligo generalizzato e indiscriminato di *retention* per la lotta alla criminalità[15].
Ed è tale complesso intrecciarsi del percorso sovranazionale con le scelte normative nazionali, nonché con l'intervento di società civile e corti interne, ad aver determinato nel tempo il formarsi – e il perdurare – di sentieri paralleli e talvolta divergenti da quello indicato dai giudici di Lussemburgo. Basti pensare alle diverse reazioni scaturite dalla pronuncia *La Quadrature du Net*: mentre il governo francese ha addirittura sottolineato la necessità di ricorrere – nella controversia dinnanzi al *Conseil d'Etat* da cui il rinvio

the permissibility of large-scale surveillance for national security purposes could be seen as a pragmatic approach of the CJEU to end the data retention saga through containing national data retention regimes by ensuring their subjection to significant safeguards and limitations so that large-scale surveillance is the exception rather than the rule», V. Mitsilegas et al., *Data retention and the future of large-scale surveillance*, cit., 17.

[13] Sul noto e articolato tema del rapporto tra libertà, diritti e garanzia della sicurezza, si rimanda, senza pretesa di esaustività, a Aa. Vv., *Convegno AIC. Libertà e sicurezza nelle democrazie contemporanee*, Padova, 2003; T. Groppi, *Democrazia e terrorismo*, Napoli, 2009; M. Cavino - M.G. Losano - C. Tripodina (a cura di), *Lotta al terrorismo e tutela dei diritti fondamentali*, Torino, 2009; C. Bassu, *Terrorismo e costituzionalismo. Percorsi comparati*, Torino, 2010; M. Bonini, *Sicurezza e tecnologia, fra libertà negative e principi liberali*, in *Rivista AIC*, 3, 2016, 1 ss.; G. De Minico, *Costituzione. Emergenza e terrorismo*, Napoli, 2016; C. Graziani, *Sicurezza e diritti in tempi di terrorismo internazionale. Tra endiadi e antitesi*, Napoli, 2022.

[14] Basti pensare alle reazioni espresse dalla ONG StateWatch che ha titolato il proprio commento alle sentenze "*A victory and a defeat for privacy*". Sotto tale profilo, «*the judgment may be seen as primarily a victory for the law enforcement community, the surveillance powers of which have been significantly expanded*», V. Mitsilegas et al., *Data retention and the future of large-scale surveillance*, cit., 10; si legga anche A. Birrer - D. He - N. Just, *The State is watching you. A cross-national comparison of data retention in Europe*, in *Telecommunications Policy*, 47, 2023, 1 ss.

[15] Queste interpretazioni "difensive" della giurisprudenza della CGUE mirano a far salva la compatibilità con la Carta di Nizza di una forma di conservazione generalizzata, alla quale nessuno Stato membro pare ancora essere disposto a rinunciare del tutto. Sul punto molto chiara è la posizione espressa ad esempio da Europol (*Proportionate data retention for law enforcement purposes*, WK 9957/2017, 21 settembre 2017) che ha criticato la realizzabilità tecnica e l'utilità di una forma di *targeted data retention*.

pregiudiziale aveva tratto origine – al concetto di "*identité constitutionnelle*" per scongiurare l'applicazione dei principi sanciti dalla CGUE nella *data retention saga*[16], il legislatore belga è invece ultimamente giunto ad approvare una disciplina che pare introdurre una forma maggiormente targettizzata di conservazione dei metadati[17], dopo che la Corte costituzionale per ben tre volte aveva dichiarato l'illegittimità della disciplina interna. O ancora si veda quanto avvenuto in Portogallo dove solo recentemente e dopo numerosi anni di attesa si è assistito all'intervento del *Tribunal Constitucional* che ha spinto ad un rinnovato e acceso dibattito sulla necessità di una novella legislazione interna ispirata ai principi determinati dai giudici eurounitari[18]. Un dibattito, questo, che, in maniera simile, si è recentemente riaperto anche in Irlanda, dopo la decisione *Dwyer*[19] e in Germania a seguito della sentenza *SpaceNet*[20].

Questo variegato insieme di sentieri diversi, fatti di provvedimenti normativi e giurisprudenziali anche molto differenti tra loro per soluzioni e tempistiche, consente certamente di individuare un tratto comune: «*the resistance from Member States to the Court's rulings highlights the political struggle between EU institutions and Member States on the future of mass surveillance*»[21]. Un futuro, quello che con difficoltà e incertezza va delineandosi, che non ha certamente visto l'apporto di un altro importante "viaggiatore": il legislatore europeo. Questo non ha fino ad ora contribuito in alcun modo alla determinazione delle tappe e della meta finale del cammino regolatorio della *data retention* e risulta anzi immobile dinnanzi al moltiplicarsi di sentieri nazionali, incapace di ricondurli ad unità e di trovare una risposta di compromesso in grado di ricongiungerli alla strada indicata dalla CGUE.

---

[16] Si fa riferimento al caso deciso dal Conseil d'Etat, 21 aprile 2021, n. 393099. Per alcuni interessanti commenti quanto alla posizione espressa dall'intervenuto governo d'Oltralpe e sulla decisione dei giudici francesi, si leggano L. Azoulai - D. Ritleng - M. Bonini, *«L'État, c'est moi»: il Consiglio di Stato francese, fra salvaguardia della sicurezza nazionale e protezione dei dati (Consiglio di Stato, Section du Contentieux, 21 aprile 2021, French Data Network e a., nn. 393099, 394922, 397844, 397851, 424717, 424718)* , in *CERIDAP*, 26 luglio 2021; J. Ziller, *Il Conseil d'Etat si rifiuta di seguire il pifferaio magico di Karlsruhe*, in *CERIDAP*, 2, 2021, 1 ss.; V. Sizaine, J.-P. Foegle, *Les fausses notes du souverainisme juridique (openedition.org)*, in *La Revue des Droits de l'Homme*, giugno 2021, 1 ss.; M. Audiber, *Conservation des donnees de connexion. Comment le Conseil d'Etat a sauve la majorité des enquete judiciaires*, in *Vielle Juridique*, 96, 2021, 16 ss.; M. Rojszcazak, *The uncertain future of data retention laws in EU: is a legislative reset possible?*, in *Computer Law and Security Review*, 41, 2021, 1 ss.; V. Mitsilegas et al., *Data retention and the future of large-scale surveillance*, cit.; A. Vedaschi, *"Customizing" La Quadrature du Net: The French Council of State, National Security and Data Retention - Brexit Institute (dcubrexitinstitute.eu)*, in *Bridge Blog*, 5 maggio 2021; N. Perlo, *La decisione del Consiglio di Stato francese sulla data retention: come conciliare l'inconciliabile*, in *Rivista di Diritti Comparati*, 2, 2021, 168 ss.

[17] Per un approfondimento sulla giurisprudenza belga nonché sugli ultimi sviluppi normativi in tema, si rinvia a C. Van de Heyning, *The Belgian Constitutional Court's data retention judgment: a revolution that wasn't*, in *Diritti comparati*, 19 aprile 2022; V. Franssen - C. Van de Heyning, *Belgium's new data retention legislation: third time lucky or three strikes and you're out?*, in E. Kosta - I. Kamara (eds), *Data retention in Europe and beyond. Law and policy in the aftermath of an invalidated directive*, Oxford, in pubblicazione (2024). Sia consentito anche di rinviare a G. Formici, *La disciplina della data retention*, cit., con specifico riferimento al capitolo dedicato al Belgio.

[18] T. Violante, *How the Data Retention Legislation Led to a National Constitutional Crisis in Portugal*, in *Verfassungsblog*, 9 giugno 2022; A. Bottacci, *Judgment n. 268/2022 of the Portuguese Tribunal Constitucional and its contribution to the European dialogue on metadata retention and access regimes*, in *European Data Protection Law Review*, 8, 2022, 412 ss.

[19] Per alcune prime riflessioni sul tema, G. Brady, *Ireland, the Dwyer Case, and the 2022 Data Retention Bill – Where do we go from here?* , in *EMILDAI Blog*, aprile 2023.

[20] Una ricostruzione della normativa tedesca e del dibattito politico ingeneratosi a seguito della sentenza *SpaceNet*, è reperibile in T. Wahl, *CJEU: German Rules on Data Retention Not in Line with EU Law*, in *Eucrim*, 15 novembre 2022.

[21] V. Mitsilegas et al., *Data retention and the future of large-scale surveillance*, cit., 3.

L'introduzione di una specifica normativa sovranazionale in materia di conservazione e acquisizione dei metadati, capace di colmare il vuoto lasciato dalla invalidazione della *Data Retention Directive*[22], non è mai stata perseguita concretamente, nonostante le tante voci che hanno raccomandato e incoraggiato un intervento in tal senso[23]. Anche la proposta di regolamento che dovrebbe sostituire l'ormai vetusta Direttiva *e-Privacy* – e, dunque, il vago art. 15 che rappresenta ad oggi l'unica disposizione sovranazionale in materia di *data retention* per scopi securitari[24] – pare lontana dall'approvazione, bloccata su questioni – tra cui la disciplina della conservazione dei metadati, appunto – rispetto alle quali Commissione, Consiglio dell'UE e Parlamento europeo non riescono al momento a trovare una visione condivisa[25].

Nell'incerto procedere del cammino regolatorio della *data retention*, qui brevemente tratteggiato, vanno allora più recentemente ad inserirsi le Conclusioni dell'Avvocato Generale Collins nel caso C-178/22; queste impongono di esaminare con attenzione il percorso tracciato dai legislatori e dalla giurisprudenza italiana nel necessario e ormai imprescindibile dialogo con la CGUE e le Istituzioni europee. Il presente contributo intende pertanto proporre una prima analisi del contesto nostrano e delle ragioni che hanno condotto al rinvio pregiudiziale del Tribunale di Bolzano; verrà poi svolta una disamina delle Conclusioni dell'Avvocato Generale, per giungere ad alcune considerazioni finali: esse apriranno a profondi interrogativi sul futuro degli strumenti di conservazione e accesso ai metadati tanto a livello nazionale quanto sovranazionale ma anche, più ampiamente, sulle sfide che i diversi "viaggiatori" sono chiamati ad affrontare dinnanzi al proliferare di sofisticati quanto insidiosi sistemi di sorveglianza massiva sempre più digitalizzati ed invasivi.

---

[22] La direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006 , riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE GU 2006 L 105/54, invalidata dalla richiamata pronuncia *Digital Rights Ireland*, non è mai stata sostituita da alcune proposta normativa volta a disciplinare a livello sovranazionale la *data retention*.

[23] In questo senso si sono espressi, ad esempio, D. Fennelly, *Data retention: the life, death and afterlife of a directive*, cit.; L. Lupária, *Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Giurisprudenza penale*, 4, 2019, 573 ss.; M. Rojszcazak, *The uncertain future of data retention laws in EU: is a legislative reset possible?*, cit. Il Consiglio dell'UE nel documento Conclusione sulla conservazione dei dati per finalità di lotta contro la criminalità, n. 9336/19 del 27 maggio 2019 aveva affidato alla Commissione il compito di avviare iniziative finalizzate a verificare l'opportunità di una apposita iniziativa legislativa *ad hoc* sulla conservazione dei metadati. L'appello all'adozione di uno strumento regolatorio comune europeo, che sia in grado di determinare una disciplina conforme alle indicazioni emerse dalla giurisprudenza della CGUE e di risolvere così le criticità derivanti dalla molteplicità di soluzioni normative sul territorio europeo, è emersa anche nel dibattito in seno alle Istituzioni europee: nel marzo 2021, infatti, il Ministro della Giustizia del Portogallo – Stato membro cui all'epoca era affidata la Presidenza del Consiglio dell'UE – aveva spinto in tale direzione.

[24] Questo articolo, come noto, attribuisce agli Stati membri una generica facoltà di deroga alla regola generale determinante la cancellazione dei metadati da parte dei *service providers*; gli Stati possono quindi disporre normative nazionali che ordinino la conservazione dei dati esterni delle telecomunicazioni per finalità – solo vagamente definite – di sicurezza nazionale, difesa, sicurezza pubblica, prevenzione, ricerca, accertamento e perseguimento di reati o di uso non autorizzato del sistema di comunicazione elettronica.

[25] Si tratta della Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM/2017/010 final. Per approfondimenti sul contenuto della proposta e valutazioni critiche della stessa, soprattutto con riferimento alla disciplina della *data retention*, si leggano le considerazioni svolte dal European Data Protection Board, *Statement 3/2021 on the e-Privacy Regulation* del 9 marzo 2021.

2. Il sentiero italiano: la normativa e la giurisprudenza nazionale dinnanzi alla giurisprudenza della Corte di giustizia dell'Unione europea

2.1. Una necessaria ricostruzione della disciplina italiana in materia di conservazione dei metadati: "l'eterno ritorno del sempre uguale"?

Se, come sopra richiamato, in altri Stati membri dell'UE le decisioni della CGUE in materia di *data retention* hanno condotto, pur con tempi e risultati non omogenei, ad un vivace dibattito politico, legislativo e giurisprudenziale, l'Italia pare invece aver intrapreso un sentiero differente.

Pur non potendo qui ripercorrere nel dettaglio tutte le tappe normative e giurisprudenziali che hanno condotto all'oggi[26], pare utile fornire alcune informazioni essenziali circa l'evoluzione della disciplina in materia: ciò consentirà di cogliere appieno il travagliato rapporto che la "via italiana" ha intessuto con il diritto dell'UE e, in special modo, con la giurisprudenza della CGUE. L'art. 132 del d.lgs. 196/2003 (d'ora in avanti Cod. Privacy) ha infatti subìto solo in tempi estremamente recenti alcune sostanziali modifiche nella direzione di una – ancora solo parziale – "conciliazione" e adattamento ai principi sanciti a livello sovranazionale nella *data retention saga*. Se dunque per anni i giudici e i legislatori nostrani sono apparsi quasi indifferenti – se non più o meno consapevolmente disattenti – alle vicende che hanno animato le riflessioni giuridiche e normative in altri ordinamenti[27], gli interventi riformatori degli ultimi anni non hanno comunque risolto dubbi interpretativi e perplessità quanto alla compatibilità della disciplina nazionale con il diritto europeo e la *case law* dei giudici di Lussemburgo. Tali permanenti dubbi hanno così trovato conferma nel rinvio pregiudiziale promosso dal Tribunale di Bolzano, che ravviva un dialogo con i giudici sovranazionali – come si dirà – raramente attivato in passato.

Procedendo allora con l'analisi della normativa di riferimento, l'art. 132 Cod. Privacy stabilisce innanzitutto un obbligo generale di conservazione dei c.d. "dati esterni delle comunicazioni" per finalità di accertamento e repressione dei reati, prevedendo una *data retention* della durata di 24 mesi per i metadati telefonici, 12 mesi per il traffico telematico e 30 giorni per le chiamate senza risposta[28].

---

[26] Per uno studio dettagliato dell'evoluzione normativa e giurisprudenziale italiana sul tema della *data retention* e acquisizione dei metadati, si rinvia a E. Andolina, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Milano, 2018; R. Flor - S. Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico*, cit.; E. Poddighe, *Art. 132*, in R. D'Orazio - G. Finocchiaro - O. Pollicino - G. Resta (a cura di), *Codice della privacy e data protection*, Milano, 2021; sia consentito anche il rinvio a G. Formici, *La disciplina della data retention*, cit., nel capitolo dedicato all'ordinamento italiano.

[27] Come rilevato da diversi autori, la giurisprudenza della CGUE in materia di *data retention* non ha suscitato, all'interno dei confini italiani, «l'interesse che meritava, né in dottrina né in giurisprudenza e soprattutto non ha turbato il sonno del legislatore nazionale», S. Marcolini, *L'istituto della data retention dopo la sentenza della CGUE del 2014*, in A. Cadoppi - S. Canestrari - A. Manna - M. Papa (a cura di), *Cybercrime*, Milano, 2019, 1591; ciò almeno sino alla sentenza CGUE, C-746/18, *H.K. v. Prokuratuur* (2021).

[28] Questa durata invero ha subìto svariate modifiche nel corso del tempo; per una ricostruzione del succedersi degli interventi normativi in materia, si rinvia a G. E. Vigevani, *Articolo* 132, in Aa. Vv., *Codice della privacy. Commento al D. Lgs. 30 giugno 2003, n. 196, aggiornato alle più recenti modifiche legislative*, Milano, 2004, 1668 ss.; C. Fatta, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*,

La disciplina della conservazione dei metadati per scopi securitari, tuttavia, non risulta essere unicamente regolata dall'art. 132 Cod. Privacy: con diversi interventi normativi, peraltro spesso disordinati e primariamente motivati da esigenze emergenziali[29], culminati da ultimo nella Legge Europea 2017[30], la "regola generale" sancita nella disposizione richiamata è divenuta *de facto* recessiva e residuale. Questo perché la Legge Europea, così come le disposizioni precedenti[31], dispone un obbligo di conservazione dei metadati in deroga a quanto previsto dal Cod. Privacy ed esteso a ben 72 mesi qualora vengano perseguiti scopi di repressione e accertamento di reati di cui agli artt. 51, c. 3-quater e 407, c. 2, lett. a) c.p.p. (terrorismo, saccheggio, associazione di tipo mafioso etc.). È questa durata di conservazione estremamente lunga e senza pari negli altri ordinamenti europei ad essere così divenuta di normale attuazione: poiché non risulta possibile conoscere in anticipo per quali obiettivi possa in futuro essere eventualmente richiesto l'accesso ai metadati, il *service provider* è tenuto a conservare tali dati in maniera generalizzata per il termine massimo di sei anni. Solo al momento della richiesta di accesso da parte dell'autorità giudiziaria, il fornitore di servizi di telecomunicazioni dovrà verificare, a seconda del reato perseguito, quale sia il periodo di conservazione relativo, ossia se quello stabilito dall'art. 132 Cod. Privacy – dunque più breve – o quello più ampio sancito dalla Legge Europea. Di conseguenza, come rilevato anche dal Garante per la Protezione dei Dati Personali, «benchè l'acquisibilità dei dati raccolti oltre il termine ordinario sia limitata a reati particolarmente gravi, proprio la natura retrospettiva di questo strumento investigativo implica la conservazione generalizzata dei dati di traffico per sei anni, salvo poi limitarne l'utilizzabilità processuale ai soli casi normativamente considerati»[32].

L'inversione del rapporto tra disciplina ordinaria e straordinaria è stata rilevata con grande enfasi anche dalla dottrina: molte sono state le critiche mosse tanto con riferimento alla tipologia di intervento normativo prescelto per modificare la regolamentazione della *data retention*, quanto sotto il profilo sostanziale. Rispetto a quest'ultimo, in particolare, sono state evidenziate la durata estremamente lunga della conservazione nonché la sua natura *de facto* generalizzata ed indiscriminata, non essendo stabilito alcun limite circa la tipologia di dati, le aree geografiche o i soggetti interessati dalla *retention*: nessuna targettizzazione della conservazione dei dati viene quindi prevista né nell'art. 132 Cod. Privacy né nelle successive modifiche intervenute

in *Diritto dell'Informazione e dell'Informatica*, 2008, 399 ss.; A. Arena, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quaderni costituzionali*, 3, 2014, 722 ss.; M. Riccardi, *Dati esteriori delle comunicazioni e tabulati di traffico. Il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore*, in *Diritto penale contemporaneo*, 3, 2016, 170 ss.

[29] Prima con il c.d. d.l. antiterrorismo (d.l. 7/2015, convertito dalla l. 43/2015) e poi con il Decreto milleproroghe del 30 dicembre 2015 (d.l. 219/2015, convertito con l. 21/2016).

[30] L. 167/2017, Legge europea che reca le disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea. Per una lettura di tale disposizione si rinvia a L. Scaffardi, La Data retention va in ascensore, in *Forum di Quaderni Costituzionali*, 28 luglio 2017.

[31] Già con il d.l. 354/2003 veniva infatti previsto per i reati di cui all'art. 407, c. 2, lett. a) c.p.p. e i delitti a danno di sistemi informatici e telematici un ampliamento del periodo di conservazione, aumentato di ulteriori 24 mesi per i dati telefonici e 6 mesi per i dati di traffico telematico rispetto a quanto disposto nell'art. 132 Cod. privacy. Anche in quel caso, come per la modifica apportata dalla Legge europea, i *service providers*, non potendo sapere in anticipo se i metadati da conservare sarebbero serviti per indagini riguardanti qualsiasi reato o solo per quelli più gravi previsti nella normativa del 2003, si trovavano costretti a conservare tutti i metadati per il termine di tempo massimo e quindi più lungo.

[32] Garante per la Protezione dei Dati Personali, *Segnalazione sulla disciplina della conservazione, a fini di giustizia, dei dati di traffico telefonico e telematico*, 2 agosto 2021.

mediante normative emergenziali. La presenza di una *bulk data retention*, peraltro significativamente prolungata, ha condotto così molti studiosi a porre in dubbio la compatibilità della legislazione italiana con il diritto dell'UE, soprattutto alla luce delle continue e coerenti pronunce dei giudici di Lussemburgo che hanno chiaramente dichiarato, come si è visto, l'illegittimità di una conservazione generalizzata per scopi di garanzia della sicurezza pubblica e repressione dei reati, quand'anche gravi[33].
Nonostante tali critiche e perplessità, però, in Italia non è mai decollato un serio dibattito sulla necessità di riformare la esaminata disciplina della *data retention*: le occasioni, anche in tempi recenti, non sono certo mancate – pensiamo alle significative modifiche apportate al Cod. Privacy all'indomani dell'entrata in vigore del regolamento UE 2016/679 (GDPR)[34] – ma il legislatore nostrano non è mai intervenuto sul profilo della conservazione dei metadati, neppure nella novella del 2021, di cui si parlerà a breve. A nulla sono valse quindi le sollecitazioni, osservabili anche con sguardo comparato e derivanti da quanto accadeva ed è accaduto in altri ordinamenti dell'UE. L'unico ambito regolatorio che ha visto il Governo e il Parlamento italiano attivarsi nella direzione di una riforma maggiormente garantista e conforme alla giurisprudenza della CGUE è quello attinente alla successiva fase dell'accesso ai metadati da parte delle autorità di indagine. Pare utile ricostruire brevemente le vicende che hanno portato a tale modifica, poiché in esse è possibile cogliere non solo un primo – tardivo – impatto della *case law* europea nell'ordinamento nostrano ma anche i semi delle questioni che emergeranno nel rinvio pregiudiziale oggetto di analisi nel presente contributo.

2.2. La novella del 2021 riguardante la disciplina dell'accesso ai metadati e il difficile dialogo promosso dalle corti nostrane con i giudici di Lussemburgo.

Prima della novella del 2021, l'art. 132 Codice Privacy attribuiva esclusivamente al p.m.

[33] «La locuzione impiegata [nell'art. 132] ricomprende qualunque reato, anche contravvenzionale e di minima gravità od offensività. Una disciplina del genere non può non contrastare con i dettami della CGUE che ha sempre affermato che il mezzo, vista la sua incidenza sul bene della riservatezza, deve applicarsi solo alla lotta contro le forme più gravi di criminalità; (..) l'obbligo italiano di conservazione universale dei dati esterni di ogni singola comunicazione elettronica effettuata da ogni cittadino, a prescindere dal suo ancorché minimo coinvolgimento in un qualsivoglia reato, per la durata di sei anni genera banche dati di sterminata dimensione, idonee a indagini e profilazioni dettagliate, ed esponendo così praticamente l'intera popolazione a quei rischi di abuso ed accesso illecito a più riprese ed accoratamente denunziati dalla giurisprudenza comunitaria. In definitiva, e senza alcun tema di smentita, la declinazione da parte del legislatore italiano delle tre variabili di conservazione dei dati esterni – i reati da contrastare, il tempo di conservazione dei dati, l'oggetto dell'obbligo di conservazione – è attualmente tra le deteriori che si possano immaginare dal punto di vista degli standard minimi di tutela della riservatezza», R. Flor - S. Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico*, cit., 47. Si leggano anche, similmente, L. Scaffardi, *La data retention va in ascensore*, cit.; L. Scudiero, *Data retention a sei anni. La Corte di Giustizia dell'UE la boccerebbe come ha fatto con l'accordo Europa Canada sui PNR*, in questa *Rivista*, 2017, 178 ss.

[34] Sul d.lgs. 101/2018 e sulle limitate e solo formali modifiche apportate in materia di *data retention* e accesso ai metadati, nelle quali si è sostanzialmente riconfermato l'assetto regolatorio precedente e sono state introdotte disposizione di coordinamento rispetto al GDPR, si veda S. Signorato, *Novità in tema di data retention. La riformulazione dell'art. 132 Codice Privacy da parte del D.Lgs. 10 agosto 2018*, in *Diritto penale contemporaneo*, 11, 2018, 157 ss. ma anche R. D'Orazio - G. Finocchiaro - O. Pollicino - G. Resta (a cura di), *Codice della privacy e data protection*, cit.

il delicato compito di vagliare e approvare le richieste di acquisizione dei metadati[35]. Inoltre, nessun limite quanto alla gravità dei reati era indicato neppure sul fronte dell'accesso, che veniva garantito per la repressione di qualsiasi tipologia di reato. La coerente e ricca *data retention saga* non aveva pertanto mai condotto, né con riferimento alla conservazione né rispetto alla disciplina dell'accesso, ad un ripensamento della normativa esistente né avevano mai posto in dubbio la compatibilità della cornice regolatoria nostrana rispetto ai principi sanciti dai giudici sovranazionali.

Un simile approccio trovava peraltro rafforzamento nella giurisprudenza nazionale, definita ormai dai più come portatrice di «orientamenti interpretativi salvifici»[36] o in altri termini, di interventi «rassicuranti», «espressione di un approccio semplicistico ad un tema (..) colmo di nodi irrisolti»[37]. Le corti italiane avevano dunque sempre optato per una lettura «restrittiva degli standard garantistici enunciati dalla CGUE» al fine di «salvare la disciplina interna (..) ed evitare ipotesi di inutilizzabilità probatoria»[38].

In questo contesto, la sentenza della CGUE *H.K. v. Prokuratuur* ha certamente rappresentato una prima significativa – per quanto parziale – spinta verso il cambiamento: tale pronuncia, pur riferendosi ad un caso estone, chiariva infatti i requisiti di terzietà ed indipendenza dei giudici o delle entità indipendenti chiamate ad effettuare il controllo preventivo all'accesso e ribadiva come quest'ultimo fosse da ritenersi limitato unicamente al perseguimento di reati caratterizzati da gravità. I profili di contatto e somiglianza tra la disciplina estone e quella italiana hanno così mosso il Tribunale di Rieti a promuovere il primo rinvio pregiudiziale azionato da giudici italiani in materia di *data retention* e accesso ai metadati[39], cui hanno inoltre fatto seguito alcune interessanti pronunce della Corte di Cassazione. Questa, pur ritenendo non direttamente applicabile la sentenza della CGUE da parte dei giudici nazionali per mancanza di autoesecutività[40], ha nondimeno dichiarato la necessità di un intervento

[35] Anche con riferimento alla disciplina riguardante l'accesso ai metadati conservati sono state disposte, nel corso del tempo, diverse modifiche normative rispetto al dettato originario dell'art. 132 Cod. privacy. Si pensi al c.d. Pacchetto Pisanu (d.l. 144/2015) che sanciva il previo controllo unicamente in capo al p.m., deputato ad emanare un decreto motivato autorizzante l'accesso ai metadati; solo in caso di reati di maggior gravità – quali quelli di cui all'art. 407, co. 1, lett. a) c.p.p. e i delitti a danno di sistemi informativi e telematici – veniva richiesta l'autorizzazione mediante decreto del giudice. Tale intervento veniva poi confermato anche dal successivo d.lgs. 109/2008, che attribuiva unicamente al p.m. il compito di autorizzare le richieste di acquisizione. Per maggiori dettagli, oltre alle fonti già richiamate in questo paragrafo, sia consentito rinviare a G. Formici, *'The three Ghosts of data retention': passato, presente e futuro della disciplina italiana in materia di conservazione e acquisizione dei metadati per scopi investigativi. Commento a margine del d.l. 30 settembre 2021, n. 132 e relativa legge di conversione*, in *Osservatorio costituzionale*, 1, 2022, 125 ss.

[36] Così R. Flor - S. Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico*, cit.

[37] L. Lupária, *Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, cit.

[38] Ivi, 757. Nel medesimo testo si può ritrovare una utile ricostruzione delle maggiori pronunce delle Corti italiane in materia.

[39] Domanda di pronuncia pregiudiziale C-334/21, promossa dal Tribunale di Rieti, Sez. Penale, Ordinanza del 4 maggio 2021 (procedimento penale contro G.B. e R.H.); tale rinvio si è tuttavia poi concluso con il ritiro della domanda di pronuncia pregiudiziale a causa della riforma normativa del 2021 che ha fatto venir meno l'utilità stessa della pronuncia dei giudici di Lussemburgo rispetto a profili regolatori nel frattempo modificati dallo stesso legislatore nazionale. Sul punto G. Stamponi Bassi, *Acquisizione dei tabulati telefonici e telematici: il Tribunale di Rieti propone questione pregiudiziale alla Corte di Giustizia dell'Unione europea*, in *Giurisprudenza Penale*, 13 maggio 2021 ma anche Ufficio del Massimario e del Ruolo, Servizio Penale della Corte Suprema di Cassazione, *Relazione su novità normativa. Misure urgenti in tema di acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale*, 13 ottobre 2021.

[40] Su questo punto invero la giurisprudenza di merito ha mostrato, prima dell'intervento della Corte

riformatore della normativa italiana in grado di tenere in debito conto i principi della giurisprudenza sovranazionale[41].

Un intervento normativo, quello invocato da più parti, che non si è fatto attendere[42]: non potendo in questa sede vagliare nel dettaglio il percorso normativo che ha condotto al d.l. 132/2021 e le modifiche apportate nella successiva legge di conversione 178/2021, ciò che qui merita innanzitutto rilevare è come il legislatore nazionale abbia apportato una modifica parziale dell'art. 132 Cod. Privacy, nella sola parte attinente alla disciplina dell'accesso, ovvero il c. 3, introducendo poi l'art. 3 bis. Il c. 1 della disposizione in esame, già analizzato precedentemente e determinante l'obbligo di conservazione, non ha invece subìto alcuna riforma – sul punto si tornerà successivamente –. Cercando di conformare la normativa italiana a quanto emerso dalla pronuncia *H.K. v. Prokuratuur*, il legislatore nostrano ha stabilito la legittimità dell'accesso ai metadati solo qualora essi siano rilevanti ai fini della prosecuzione delle indagini nonché quando vi siano sufficienti indizi in ordine a determinate tipologie di reati considerati "gravi". Questi sono individuati nei reati per i quali la legge stabilisce la pena dell'ergastolo o la reclusione non inferiore nel massimo a tre anni – a norma dell'art. 4 c.p.p. – e nei reati di minaccia, molestia o disturbo gravi alle persone col mezzo del telefono. Oltre a queste importanti ed inedite restrizioni, anche il soggetto deputato a vagliare e autorizzare l'accesso è stato modificato, in conformità a quei criteri di indipendenza e terzietà emersi con maggior chiarezza dalla sentenza *H.K. v. Prokuratuur*: i metadati devono ora essere acquisiti sulla base di un decreto motivato del giudice, su richiesta del p.m. o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e di altre parti private[43]. In estrema sintesi, l'intervento del legislatore ha inserito, per la prima volta, una soglia di pena oltre la quale il reato è considerato grave – e quindi in grado di legittimare una ingerenza grave nella sfera personale – e ha altresì innalzato il livello di tutela dei soggetti colpiti dall'accesso prevedendo un intervento del giudice e non del p.m. a scopi autorizzativi preventivi.

Se quanto disposto va certamente nella direzione di un maggior garantismo ed

di Cassazione, approcci ondivaghi e talvolta confliggenti, come emerge ad esempio dalla Tribunale di Milano, VII Sez. Penale, ord. 22 aprile 2021, n. 585 e dal Tribunale di Roma, Sez. G.i.p.-G.u.p., decreto 25 aprile 2021. Su tali pronunce, si rimanda alle valutazioni critiche di J. Della Torre, *L'acquisizione dei tabulati telefonici dopo la Corte di Giustizia: un primo provvedimento garantista del gip di Roma*, in *Sistema Penale*, 29 aprile 2021; C. Parodi, *Tabulati telefonici e contrasti interpretativi: come sopravvivere in attesa di una nuova legge*, in *ilPenalista*, 3 maggio 2021; A. Malacarne, *Ancora sulle ricadute della CGUE in tema di data retention: il G.i.p. di Roma dichiara il "non luogo a provvedere"* , in *Sistema Penale*, 5 maggio 2021; V. Tordi, *Data retention dopo la CGUE: Trib. Milano nega il contrasto della disciplina italian con il diritto sovranazionale*, in *Sistema Penale*, 7 maggio 2021; F. Torre, *Data retention: una ventata di "ragionevolezza" da Lussemburgo*, in *Consulta Online*, II, 2021, 540 ss.; ma anche A. Ciprandi, *La Cassazione sull'utilizzabilità dei tabulati acquisiti prima del DL 132/2021*, in *Sistema Penale*, 22 febbraio 2022.

[41] Nella sentenza n. 33116 del 7 settembre 2021, similmente a quanto già statuito nella pronuncia n. 28523 del 22 luglio 2021, la Corte di Cassazione ha ritenuto la sentenza *H.K. Prokuratuur* non direttamente applicabile dai giudici nazionali per mancanza di auto-esecutività. Il riconoscimento della importanza di una modifica della normativa vigente si pone in discontinuità rispetto alla previgente giurisprudenza delle Corti italiane (ad es. rispetto all'Ordinanza del Tribunale di Padova del 15 marzo 2017, Pres. Marassi o alla sentenza del 25 settembre 2019, n. 48737 della Cassazione stessa).

[42] L'Ordine del giorno 9/2670-A/10 del 1° aprile 2021, adottato dal Governo italiano, dimostra l'attenzione rinnovata e l'impegno a riformare la normativa nazionale all'epoca vigente sulla base dei principi sanciti dalla giurisprudenza della CGUE.

[43] Viene prevista una disciplina d'urgenza che consente al p.m. di disporre direttamente l'acquisizione dei metadati mediante proprio decreto, che deve tuttavia poi essere oggetto di apposita convalida.

attenzione ai requisiti sanciti a livello sovranazionale, interrompendo quella indifferenza e "disattenzione" caratterizzante la giurisprudenza ma anche il dibattito normativo italiano fino a quel momento, la riforma delineata ha nondimeno fatto sorgere alcune valutazioni critiche. Se ne vogliono riportare solo alcune, utili anche a comprendere la posizione assunta dal giudice di Bolzano nel rinvio pregiudiziale oggetto di analisi. Innanzitutto, dubbi sono emersi quanto alla soglia di gravità indicata: essa finisce invero col ricomprendere la gran parte dei delitti inseriti nel codice penale, così che la disposizione novellata darebbe solo «l'illusione di aver effettuato una delimitazione del perimetro delle violazioni ma in realtà non lascia fuori che le contravvenzioni e pochi delitti di davvero infima gravità»[44]. Inoltre non è mancato chi ha scorto nella determinazione in via astratta e generale di una soglia di pena, oltrepassata la quale si produce una «presunzione assoluta di proporzionalità, indipendentemente dalla valutazione del caso concreto», una soluzione incapace di rispondere ai profili di incompatibilità con il diritto eurounitario; dovrebbe, al contrario, essere «assolutamente indispensabile integrare la valutazione effettuata dal legislatore con quella operata dal giudice in concreto, valutando le peculiarità del caso di specie ed utilizzando i parametri indicati nel nuovo art. 132 (sussistenza dei sofficienti indizi di reato e rilevanza ai fini della prosecuzione delle indagini)»[45].

Ebbene proprio dai limiti e criticità[46], emersi all'indomani della riforma promossa dal legislatore nazionale, ha avuto origine il rinvio pregiudiziale che ci si appresta ad esaminare, nel quale è possibile ravvisare un primo e più significativo allontanamento – la cui portata è però ancora tutta da verificare – dalla previa interpretazione "salvifica" della normativa nazionale assunta dalle corti nostrane in passato.

Il caso da cui il rinvio prende le mosse trae origine da due procedimenti penali per furto aggravato di telefoni cellulari, nel corso dei quali il p.m. della Procura di Bolzano aveva avanzato al giudice del Tribunale richiesta di accesso a tutti i metadati conservati dalle compagnie telefoniche, relativi ai due dispositivi rubati[47]. Sulla base del già richiamato art. 132 Cod. Privacy, modificato dal d.l. 132/2021, i reati di cui agli artt. 624 e 625

---

[44] R. Flor - S. Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico*, cit., 54.

[45] F. Zani, *L'ingerenza nel diritto fondamentale alla vita privata ed alla riservatezza alla luce della recente sentenza della Corte di Giustizia 2 marzo 2021 tra principi dell'Unione europea e principi costituzionali*, in *Osservatorio costituzionale*, 6, 2021, 482.

[46] Sul punto, per una ampia e puntuale riflessione sull'evoluzione normativa in tema di *data retention*, si legga A. Malacarne - G. Tessitore, *La ricostruzione della normativa in tema di data retention e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?*, in *Archivio penale*, 3, 2022, 1 ss. Si consenta di rinviare altresì a G. Formici, *'The three Ghosts of data retention'*, cit., per una disamina delle posizioni, anche critiche, espresse dalla dottrina all'indomani della approvazione del d.l., soprattutto con riferimento all'introduzione del vaglio preventivo in capo al giudice e non più al p.m. e alla determinazione della soglia di gravità. Si fa riferimento alle posizioni espresse, tra gli altri, da F. Filippi, *La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi* , in *Penale. Diritto e procedura*, 1 ottobre 2021; G. Amato, *Nella costruzione normativa si è sminuito il ruolo del p.m.*, in *Guida al diritto*, 39, 2021, 22 ss.; F. Rinaldini, *La nuova disciplina del regime di acquisizione dei tabulati telefonici e telematici: scenari e prospettive*, in *Giurisprudenza penale*, 10, 2021, 1 ss.; G. Pestelli, *D.L. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonici e telematici,* in *Quotidiano giuridico*, 4 ottobre 2021; V. Palladini, *Data retention e privacy in rete: verso una regolazione conforme al diritto UE?*, in *Rivista italiana di informatica e diritto*, 1, 2022, 103 ss.

[47] In particolare, si fa riferimento a «utenze ed eventualmente codici IMEI chiamati/chiamanti, siti visitati/raggiunti, orario e durata della chiamata/connessione ed indicazione delle celle e/o ripetitori interessati, utenze ed IMEI mittenti/destinatari degli SMS o MMS e, ove possibile, generalità dei relativi destinatari) delle conversazioni/comunicazioni telefoniche e connessioni effettuate, anche in roaming, in entrata e in uscita anche se chiamate prive di fatturazione (squilli) dalla data del furto fino alla data della elaborazione della richiesta».

c.p. rientrano nel novero dei reati "gravi", essendo per gli stessi stabilita una pena di reclusione non inferiore nel massimo a tre anni.
Dinnanzi a tale disposizione, come attuata nel caso concreto, tuttavia, il giudice di Bolzano ha mostrato rilevanti perplessità quanto alla conformità rispetto al diritto dell'UE, come interpretato dalla CGUE, soprattutto nelle pronunce *Ministerio Fiscal* e *H.K. Prokuratuur*. In queste decisioni, infatti, viene ribadito con chiarezza come l'accesso a dati che consentono di trarre precise conclusioni sulla vita privata di un utente costituisca una grave ingerenza nei diritti fondamentali, in particolare quelli di cui agli artt. 7, 8 e 52 della Carta di Nizza. Una tale significativa compressione dei diritti e delle libertà dovrebbe pertanto essere legittimata unicamente dal perseguimento di obiettivi di lotta alla criminalità *grave* e solo a condizione che l'accesso sia subordinato a forme di controllo preventivo da parte di un giudice o di una entità amministrativa indipendente[48]. Considerando tali principi, a parere del giudice di Bolzano il limite edittale sancito dal novellato art. 132 Cod. Privacy, finirebbe, come nel caso concreto, per consentire una ampia acquisizione di tabulati telefonici anche per reati che, nella realtà dei fatti, «destano scarsissimo allarme sociale»[49] e mancano di quel necessario elemento di gravità affermato nella *case law* sovranazionale.
Il giudice italiano, sulla base della normativa interna, si troverebbe inoltre *obbligato*, secondo la lettura del Tribunale del rinvio, ad autorizzare l'accesso ai metadati ogniqualvolta ricorrano le condizioni sancite dall'art. 132 (sufficienti indizi di reato e rilievo dei dati ai fini dell'accertamento del reato), senza poter esercitare, cioè, alcuna valutazione specifica sulla concreta gravità del reato nella fattispecie realizzata. L'approvazione della richiesta di acquisizione risulterebbe quindi imposta in caso di raggiungimento della sola soglia di gravità sancita dal legislatore in maniera astratta, esulando dalla considerazione della reale gravità del reato perseguito e di quel nesso conseguenziale e di proporzionalità individuato tra la ingerenza significative nella sfera privata e il necessario perseguimento di un reato dotato di carattere di gravità.
Sulla base di tali valutazioni, che paiono peraltro tenere in conto quelle riflessioni critiche avanzate anche dalla dottrina all'indomani della riforma normativa e più sopra richiamate, il giudice di Bolzano ha deciso quindi di rimettersi alla CGUE affinché questa possa esprimersi «in ordine alla questione se l'art. 15 direttiva 2002/58/CE, così come interpretato nella sentenza C-746/18, osti ad una normativa nazionale che genericamente e senza differenziare tra i vari tipi di reato impone, in presenza di sufficienti indizi di reato, l'acquisizione dei tabulati telefonici per reati puniti con una pena non inferiore nel massimo a tra anni di reclusione e la multa»[50].

---

[48] *Ex multis*, per una lettura approfondita della pronuncia *H.K. v. Prokuratuur*, si veda I. Revolidis, *H.K. v. Prokuratuur: on balancing crime investigation and data protection (Opinion og AG Pitruzzella)*, in *European Data Protection Law Review*, 2, 2020, 319 ss.; E. Andolina, *Ancora una pronuncia della Grande Camera della Corte di Giustizia UE in tema di condizioni di accesso ai traffic data*, in *Processo penale e giustizia*, 5, 2021, 1204 ss.; S. Rovelli, *Case Prokuratuur: proportionality and the independence of Authorities in data retention*, in *European Papers*, 1, 2021, 199 ss.; B. Brunessen, *Chronique Droit européen du numérique. Les précisions sur l'interprétation et l'application du régime de l'e-privacy*, in *Revue trimestrielle du Droit européen*, 3, 2022, 481 ss.; G. Naddeo, *Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella "data retention saga" dinanzi alla Corte di giustizia*, in *Freedom, security & justice : european legal studies*, 2, 2022, 188 ss.; sia consentito anche il rinvio a G. Formici, *La sentenza H.K. c. Prokuratuur e il difficile dialogo tra CGUE e Stati membri in materia di conservazione e accesso ai metadati per finalità securitarie*, cit.

[49] Come si legge nell'Ordinanza di domanda di pronuncia pregiudiziale alla Corte di giustizia dell'UE (art. 267 TFUE) disposta dal Tribunale di Bolzano, Giudice delle indagini preliminari, RGNR 9794/ignoti 2021 e RGNR 9228/ignoti 2021.

[50] *Ibidem*.

3. La direzione indicata dalle Conclusioni dell'Avvocato Generale Collins nel caso C-178/22

Nelle sue Conclusioni, l'Avvocato Generale ripercorre utilmente i principi e requisiti di proporzionalità e necessità indicati dalla CGUE nella sua costante giurisprudenza; con riferimento, in particolare, ai metadati di traffico e localizzazione, in grado di rintracciare e identificare fonte e destinazione di una comunicazione, viene ribadito quanto già precisato nelle pronunce *Ministerio Fiscal* e *H.K. v. Prokuratuur*: la necessaria sussistenza di un reato grave per giustificare l'accesso a metadati in grado di fornire informazioni precise sulla vita dell'utente e quindi determinanti una ingerenza grave nei diritti alla riservatezza e alla protezione dei dati[51].

È proprio partendo da tali premesse che l'Avvocato Generale Collins legge il rinvio del Tribunale di Bolzano come la richiesta di un chiarimento e una maggior specificazione tanto della nozione di gravità del reato quanto del tipo di controllo *ex ante* che l'autorità giudiziaria è chiamata a svolgere dinnanzi a disposizioni nazionali, come quelle di cui all'art. 132 Cod. Privacy italiano, che impongono di autorizzare l'accesso qualora il reato superi la soglia di gravità stabilita dal legislatore stesso.

Ecco allora che l'Avvocato Generale osserva innanzitutto come né la Direttiva *e-Privacy* né la giurisprudenza della CGUE forniscano alcuna nozione del termine "reato" e tanto meno di "reato grave". Ne deriva, come sostenuto anche dalla Commissione e dagli Stati membri che hanno presentato osservazioni alla Corte, che sia da porsi in capo ai legislatori nazionali il compito di definire i reati che consentono l'accesso ai metadati. Ciò anche riconoscendo che «la definizione dei reati e delle sanzioni

[51] Del resto il caso *Ministerio Fiscal* presenta talune somiglianze e punti di incontro nonché alcune distinzioni rispetto ai fatti e alle questioni giuridiche poste alla base del rinvio italiano in esame: anche nelle vicende spagnole, infatti, le indagini prendevano avvio dal furto di un cellulare. In quell'ordinamento, tuttavia, diversamente da quanto disposto dalla normativa italiana vigente, il furto non rientrava nella definizione di "reato grave" fornita dal legislatore nazionale che fissava la soglia di gravità in caso di pena detentiva superiore a 3 anni, non intercorrente nel caso di specie. Il giudice istruttore spagnolo, quindi, si trovava nella condizione di dover negare l'emanazione dell'ingiunzione volta all'accesso ai metadati – e in particolare quelli identificativi – richiesta dalla polizia investigativa. Dinnanzi a tale situazione, il giudice del rinvio si era però chiesto se la normativa nazionale fosse compatibile con i principi fissati dal diritto dell'UE con riferimento al requisito della gravità del crimine legittimante l'intrusione nella sfera privata. Ebbene, in quel caso la CGUE non si era spinta – come si dirà anche a breve – ad identificare e specificare i criteri di determinazione della gravità del reato bensì aveva affermato un solo primo rilevante principio: i giudici nazionali, dinnanzi alla richiesta di accesso ai metadati, sono chiamati a valutare innanzitutto se la compressione dei diritti fondamentali sia di gravità e profondità tale da richiedere la sussistenza di un reato grave. Nello specifico caso spagnolo i dati richiesti dalla polizia non riguardavano né la localizzazione né i dettagli delle comunicazioni svolte, bensì si limitavano esclusivamente ai dati identificativi dei titolari di carte SIM attivate con il telefono rubato, che venivano richiesti peraltro per un arco di tempo estremamente limitato. Considerati tali profili, la CGUE aveva rinvenuto un'ingerenza non grave nella sfera privata dei soggetti potenzialmente colpiti dall'accesso, così che non si rendeva necessaria la sussistenza di un obiettivo di lotta alla criminalità grave al fine di concedere l'acquisizione dei dati. Oltre a questo vaglio di proporzionalità, i giudici di Lussemburgo non mancavano però di indicare alcuni principi e considerazioni di rilievo anche per il rinvio italiano e infatti ripresi nelle Conclusioni qui analizzate: in primis che i dati relativi a traffico ed ubicazione permettono di ricostruire abitudini, relazioni sociali e frequentazione di luoghi dei soggetti interessati, rappresentando così una ingerenza grave rispetto alla quale a nulla rilevano considerazioni quanto alla durata del periodo per il quale l'accesso viene richiesto o alla quantità di dati acquisiti. La CGUE ha infatti ribadito come anche l'accesso ad un quantitativo limitato di dati o per un breve periodo soltanto risulti comunque idoneo a trarre informazioni precise sulla vita privata dell'utente, tali da richiedere quindi la sussistenza di un reato grave. Queste valutazioni sono certamente di estrema importanza per guidare il giudice o l'autorità amministrativa indipendente nella fase di vaglio di proporzionalità e controllo preventivo.

riflette le sensibilità e le tradizioni nazionali, che variano notevolmente non soltanto da uno Stato membro all'altro, ma anche nel corso del tempo, parallelamente rispetto alle trasformazioni della società», § 28. Gli Stati membri, dunque, sono competenti a definire i criteri di gravità nelle proprie normative nazionali in materia di *data retention* e accesso ai metadati.

Occupandosi, in tale contesto, del residuale ruolo di controllo esercitabile dal giudice dinnanzi alla richiesta di accesso, l'Avvocato Generale propone un ragionamento articolato che merita qui di essere analizzato con attenzione. Sulla base della sentenza *H.K. v. Prokuratuur*, innanzitutto, viene riaffermato come la deroga alla riservatezza dei dati di comunicazione debba rappresentare una eccezione e non una regola generale: l'interpretazione restrittiva dell'art. 15 Direttiva *e-Privacy* impone di conseguenza che vengano rispettati i principi di equivalenza, effettività e proporzionalità, così che «l'obiettivo della lotta contro la criminalità grave deve sempre essere conciliato con il godimento dei diritti fondamentali in tal modo pregiudicati», § 32. Le disposizioni nazionali in materia devono pertanto consentire e prevedere non solo un controllo preventivo da parte di un'autorità giudiziaria o amministrativa indipendente ma anche che l'autorità così individuata «concili i diversi interessi e diritti in gioco, al fine di garantire un giusto equilibrio tra le necessità di indagine e della salvaguardia dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali degli interessati», § 33. È da questa considerazione che l'Avvocato Generale fa derivare le sue considerazioni sul ruolo del giudice, partendo però da una premessa rilevante: la legge italiana fissa in modo chiaro e preciso le condizioni alle quali il giudice deve consentire l'accesso ai dati (§ 34); in linea generale, e sempre considerando la norma nazionale in astratto, l'Avvocato Generale si spinge infatti ad affermare che «sebbene l'art. 132 riguardi, potenzialmente, un'ampia gamma di reati, la Corte [di giustizia dell'UE] non dispone, nell'ambito del presente procedimento, di alcun elemento idoneo a dimostrare che in esso ricada un numero talmente elevato di reati da rendere l'accesso ai dati ai sensi di tale disposizione la regola anziché l'eccezione. La soglia della reclusione non inferiore nel massimo a 3 anni non appare eccessivamente bassa», § 35.

Nonostante questa valutazione, l'Avvocato Generale si affretta però ad evidenziare come sia necessario osservare anche l'applicazione pratica e concreta dell'art. 132. Quest'ultimo stabilisce l'obbligo di autorizzazione dell'accesso ai metadati qualora tali informazioni «siano rilevanti per l'accertamento dei fatti e sussistano sufficienti indizi della commissione di un reato di minaccia e di molestia o disturbo alle persone per mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi» § 36) o della commissione di reati puniti, segnatamente, con la pena della reclusione non inferiore nel massimo a tre anni (§ 38). Secondo la lettura dell'Avvocato Generale, è possibile così identificare due distinti livelli di controllo preventivo che il giudice italiano è chiamato ad operare: nel primo caso, quando cioè sussiste un reato di minaccia e di molestia o disturbo alle persone per mezzo del telefono, viene richiesta una valutazione individuale, nel caso concreto, «della questione se l'ingerenza nei diritti sia proporzionata rispetto all'obiettivo di interesse generale della lotta contro la criminalità», § 36. Qualora invece si tratti della commissione di reati puniti con la pena della reclusione non inferiore nel massimo a tre anni, il giudice si trova limitato a stabilire solamente «che i requisiti oggettivi ricorrano, senza alcuna possibilità di effettuare una valutazione individuale degli interessi in gioco», § 38. I giudici nazionali, in tal caso, non parrebbero quindi essere competenti a sindacare e mettere in discussione la determinazione della soglia di gravità stabilita dal legislatore, che da sola basterebbe a limitare la valutazione e il ruolo del giudice nel concedere l'autorizzazione.

Su tale specifico punto l'Avvocato Generale giunge ad una considerazione di grande importanza: i giudici devono «*in ogni caso* essere competenti a effettuare una valutazione individuale" quanto alla proporzionalità della concessione dell'accesso (..) a dati sensibili che consentono di trarre precise conclusioni sulla vita privata dell'utente», § 39 (corsivo aggiunto). In questo modo, anche nel caso in cui sussista una soglia di gravità sancita per via legislativa, deve essere lasciato in capo ai giudici non tanto – o non solo – il compito di sancire il raggiungimento della gravità stabilita per legge, bensì – e questo è ciò che interessa maggiormente – l'onere di svolgere una valutazione o controllo individuali sulla proporzionalità della ingerenza rispetto all'obiettivo di lotta contro la criminalità nel caso concreto (§ 40). Ne consegue che «in taluni casi, l'accesso a siffatti dati può essere negato anche qualora il reato raggiunga la soglia di gravità prevista dal diritto nazionale» (§ 40), così lasciando un ruolo importante di discrezionalità e di considerazione concreta all'autorità di controllo, che non deve ritenersi in toto vincolata alle considerazioni del legislatore. Nel caso, quindi, in cui la soglia di gravità fissata per legge non venga raggiunta, il giudice del rinvio non potrà concedere l'accesso ai dati. Nel caso però in cui tale soglia sia superata, il giudice non è obbligato ad autorizzare l'accesso ma deve piuttosto controllare se «alla luce di tutte le circostanze che caratterizzano lo specifico caso di cui trattasi, l'ingerenza nei diritti fondamentali determinata dalla concessione dell'accesso (..) sia proporzionata all'obiettivo di interesse generale della lotta contro tale reato», § 42.

Nel caso concreto a lui sottoposto dal giudice italiano, l'Avvocato Generale sembra suggerire di considerare, ai fini della determinazione di questo rapporto di proporzionalità, tutti i diritti e gli interessi pertinenti, «compresi, segnatamente, i danni causati ai diritti di proprietà delle vittime tutelati dall'art. 17 della Carta [di Nizza], nonché il fatto che i telefoni cellulari possono contenere informazioni altamente sensibili relative alla vita privata, professionale e finanziaria dei loro proprietari. L'accesso ai dati in parola può inoltre essere l'unico mezzo efficace disponibile per indagare e perseguire i reati di cui trattasi e per garantire che i loro autori, al momento ignoti, non restino impuniti. Anche i diritti dei terzi devono essere presi in considerazione» (§ 42), valutando ad esempio, per quanto attiene ai diritti dei terzi – quali le vittime del reato –, se l'accesso ai dati è ristretto nel tempo e se sussistono garanzie processuali nel diritto italiano volte ad assicurare sia la distruzione di tutti i dati che, a seguito dell'accesso, non siano utili al fine dell'individuazione degli autori del furto, sia l'impossibilità di utilizzare i dati acquisiti in violazione dell'art. 132 Cod. Privacy.

Ne deriva, pertanto, come il diritto dell'UE non osti a una legge nazionale «che impone al giudice di autorizzare il p.m. ad accedere a dati legittimamente conservati dai fornitori (..) che consentono di trarre precise conclusioni sulla vita privata di un utente, qualora i dati siano rilevanti per l'accertamento dei reati e sussistano sufficienti indizi della commissione di un reato grave, come definito dal diritto nazionale, punito con la pena della reclusione non inferiore nel massimo a 3 anni. Prima di concedere l'accesso, il giudice nazionale deve effettuare una valutazione individuale della questione se l'ingerenza nei diritti fondamentali (..) sia proporzionata, alla luce, segnatamente, della gravità del reato in discussione e dei fatti del caso di cui trattasi», § 44.

Se, in definitiva, viene confermata la legittimità della scelta del legislatore italiano quanto alle condizioni e alla soglia di gravità individuata, viene al contempo lasciato un margine di valutazione al giudice che deve svolgere le proprie considerazioni quanto alla proporzionalità dell'ingerenza, indipendentemente – e quindi non esclusivamente – dal raggiungimento della soglia di gravità del reato. Ne emerge un rafforzamento del potere attribuito ai giudici, perché l'autorizzazione all'accesso resta comunque subordinata al

controllo di proporzionalità svolto dai giudici stessi. Una interpretazione del diritto dell'UE e della previa giurisprudenza della CGUE che lascia quindi un significativo margine di azione ai giudici nel controllo *ex ante* e che consente di limitare la rigidità della scelta del legislatore nazionale nella definizione di gravità del reato.

4. Tante tappe ma quale meta? La difficoltà di scorgere un punto di arrivo

Nella decisione qui analizzata sono presenti senza dubbio forti elementi di continuità con la giurisprudenza elaborata dalla CGUE, soprattutto con riferimento alle pronunce *Ministerio Fiscal* e *HK v. Prokuratuur*: il parallelismo tra gravità dell'ingerenza e gravità del reato viene riaffermato con chiarezza e viene individuato come il primo necessario vaglio da effettuare nella fase di accesso ai metadati. Solo in caso di ingerenza grave, che è da riscontrarsi qualora la quantità e qualità dei metadati richiesti siano tali da rivelare informazioni precise sulla vita dell'utente, si renderà necessaria la sussistenza di un reato grave.
L'Avvocato Generale Collins, tuttavia, sembra aggiungere un ulteriore tassello a questa già nota ricostruzione: verrebbe meno, infatti, la correttezza assoluta dell'equazione "gravità dell'ingerenza + gravità del reato = concessione dell'autorizzazione all'accesso". In altri termini, ciò che viene messo in discussione è quell'automatismo che vedrebbe il giudice obbligato ad assicurare l'accesso ai metadati sulla base del mero raggiungimento della soglia di gravità del reato perseguito. Se il carattere di gravità predeterminato dal legislatore è certamente una delle condizioni necessarie alla concessione dell'accesso, esso non dovrebbe essere il solo ed unico: va sommato, piuttosto, ad un controllo individuale del giudice – o dell'autorità amministrativa indipendente – volto a determinare la proporzionalità dell'ingerenza rispetto all'obiettivo di interesse generale, con riferimento allo specifico caso concreto e considerati tutti gli elementi di fatto e gli interessi in gioco.
In questo senso, le Conclusioni dell'Avvocato Generale valorizzano certamente il ruolo del giudice e la profondità del vaglio preventivo, consentendo di raggiungere esiti diversi: concedere l'acquisizione dei metadati di localizzazione e ubicazione – determinanti quindi una ingerenza grave – anche per reati che, pur superando la soglia di gravità determinata per legge, non destino particolare allarme sociale, qualora l'ingerenza sia proporzionata all'interesse perseguito; o, al contrario, negare l'accesso, anche in presenza di reato grave, nel caso in cui non sussista un interesse pubblico tale da giustificare l'ingerenza nella sfera personale. Questo ulteriore vaglio potrebbe allora risultare in un approccio maggiormente garantista dei diritti fondamentali, permettendo di prendere in considerazione i fatti concreti e determinando così la possibilità di limitare l'accesso ai metadati anche quando il legislatore nazionale abbia individuato una soglia estremamente bassa di gravità. In questa situazione, l'ulteriore e aggiuntivo vaglio di proporzionalità del giudice potrebbe contribuire a correggere le distorsioni derivanti dall'utilizzo del criterio di gravità quale unico e vincolante elemento di valutazione ai fini dell'acquisizione. Ovviamente un simile esito in senso maggiormente garantista, dipenderebbe in ogni caso dal livello di approfondimento e attenzione dedicato al vaglio di proporzionalità ulteriore. Le Conclusioni dell'Avvocato Generale finiscono, pertanto, col limitare il valore della scelta normativa generale ed astratta del decisore politico, per riconoscere un aggiuntivo livello di tutela rappresentato dal controllo *ex ante*.

Nulla viene detto, invece, quanto alla determinazione dei criteri che i legislatori dovrebbero considerare per individuare la soglia di gravità del reato: questo profilo, del resto, non era stato toccato nemmeno nel caso *Ministerio Fiscal*, nel quale pure il giudice del rinvio aveva espressamente promosso un quesito sul punto. In quel caso l'Avvocato Generale Saugmandsgaard Øe si era spinto a fornire alcune indicazioni in merito[52], poi non riprese tuttavia nella decisione della CGUE. Nelle Conclusioni in esame, invece, viene solo ribadito come la determinazione della gravità non possa risultare nel tramutare l'eccezione in regola, determinando cioè una soglia così bassa da includere *de facto* tutti i reati previsti dall'ordinamento e facendo venir meno il significato stesso del requisito di gravità. In assenza di disposizioni a livello sovranazionale che forniscano una definizione di "reato grave", tale onere viene poi riconosciuto in capo agli Stati membri che, per tale determinazione, possono tenere conto di diversi fattori, in misura variabile, tra i quali certamente emerge con evidenza la gravità della sanzione prevista[53].
Dinnanzi a tali considerazioni derivanti dalla lettura delle presenti Conclusioni, è possibile ora trarre due ordini di riflessioni: una prima riferita specificamente all'ordinamento italiano e una seconda, più ampia, sul possibile futuro della *data retention* nell'UE.
Partendo dal primo profilo, non si può che rilevare come le Conclusioni dell'Avvocato Generale, qualora confermate dalla CGUE, possano rappresentare l'occasione per rivitalizzare il dibattito nostrano in materia di conservazione e accesso ai metadati. In particolare, il riconoscimento della facoltà, in capo ai giudici, di effettuare un vaglio capace anche di slegarsi dalla valutazione della mera soglia di gravità imporrebbe di ripensare il novellato art. 132 Cod. Privacy, con specifico riferimento alla prevista obbligatorietà della concessione dell'acquisizione dei metadati in base alla mera sussistenza dei requisiti definiti nella disposizione. Una tale riflessione dovrebbe condurre ad una interpretazione – o una riscrittura – della normativa stessa in grado di affermare con chiarezza una maggiore discrezionalità del giudice e un margine valutativo ampio quanto alla proporzionalità dell'accesso nel caso concreto. Ciò andrebbe peraltro a corroborare talune critiche, inizialmente avanzate da parte della dottrina, che mettevano in guardia quanto alla correttezza e compatibilità con il diritto dell'UE di valutazioni e controlli unicamente fondati sui criteri astratti determinati dal legislatore e che rivendicavano quindi il potere del giudice di vagliare anche le circostanze del caso concreto[54] ai fini della concessione o meno dell'autorizzazione.
Se simili analisi potranno certamente promuovere un dibattito futuro e una possibile

[52] Nel caso CGUE, C-207/16, *Ministerio Fiscal* (2018), la CGUE, riformulando il quesito posto dal giudice del rinvio, non era giunta ad affrontare la questione attinente alla individuazione dei criteri di gravità dei reati. L'Avvocato Generale, invece, aveva svolto valutazioni in tal senso, affermando innanzitutto come non fosse possibile fissare una soglia di gravità così bassa «da far diventare principio l'eccezione», § 114, negando poi la natura di nozione autonoma del diritto dell'UE della definizione di "reato grave" e quindi fornendo solo in subordine alcune indicazioni e criteri sulla base dei quali fondare la valutazione di gravità (§ 105). Secondo l'Avvocato Generale, quest'ultima non dovrebbe comunque basarsi unicamente sul *quantum* della pena e dunque su un criterio meramente formale (§ 121); veniva infine evidenziato come la soglia suddetta non dovesse essere determinata in via giurisprudenziale: «poiché una simile determinazione richiede una valutazione complessa e potenzialmente soggetta a evoluzione, occorre a mio avviso restare prudenti a questo proposito e riservare tale operazione alla valutazione dei legislatore dell'Unione, nella sfera delle competenze conferite a quest'ultima, o alla valutazione del legislatore di ciascuno Stato membro, entro i limiti dei requisiti derivanti dall'Unione», § 117.

[53] «La durata di una pena detentiva può riflettere l'analisi di una serie di fattori tra i quali la gravità intrinseca percepita di un reato e la sua gravità relativa rispetto ad altri reati», § 29.

[54] Sul punto si rinvia alle riflessioni critiche di F. Zani, *L'ingerenza nel diritto fondamentale alla vita privata ed alla riservatezza alla luce della recente sentenza della Corte di Giustizia 2 marzo 2021 tra principi dell'Unione europea e principi costituzionali*, cit.

riforma della disciplina nazionale vigente in materia di acquisizione dei metadati, non può non essere evidenziato come tale disamina critica sia unicamente limitata al profilo dell'accesso. Il giudice del rinvio, infatti, nulla ha detto – né ha interrogato la CGUE – quanto alla fase previa di conservazione e alla disciplina che la regola: nessun profilo di problematicità, insomma, è stato identificato con riferimento ad un obbligo di conservazione che rimane generalizzato e indiscriminato e che rappresenta, quindi, a parere di molti, la «violazione più grave»[55] operata dalla normativa italiana rispetto al diritto dell'UE, tanto sotto il fronte della estensione della *retention* – tutto fuor che targettizzata –, quanto della durata, macroscopicamente sproporzionata e lontana dalle soluzioni normative adottate – o in corso di discussione – in altri ordinamenti[56].

Un commento delle Conclusioni dell'Avvocato Generale Collins nel caso analizzato non può, in tal senso, esimersi da una considerazione più approfondita del contesto italiano e delle problematicità riguardanti la normativa attuale in materia di *data retention*: se l'intervento riformatore del 2021 ha senza dubbio il pregio di aver – per la prima volta – osservato con serietà la giurisprudenza della CGUE[57], esso è nondimeno caratterizzato da modifiche "selettive", riguardanti solo un aspetto determinato – quello dell'accesso. Ignorando i moniti del Garante per la Protezione dei Dati Personali[58], la scelta del Governo, prima, e del Parlamento, poi, è stata quella di avviarsi per un sentiero ancora significativamente lontano da quello segnalato dalla giurisprudenza dei giudici di Lussemburgo. Sebbene la direzione di tale ultimo percorso sia ancora difficile da determinare con chiarezza, come si dirà a breve, il compito del legislatore nazionale dovrebbe nondimeno essere quello di promuovere – grazie anche all'impulso della società civile e delle corti – un dibattito attento, capace di considerare quei principi e requisiti già indicati dalla CGUE e verso i quali sempre più Stati membri – certo, non senza difficoltà – stanno cercando di tendere. Stimolare una riflessione più ampia e complessiva sulla disciplina della *data retention* e dell'acquisizione dei metadati, che prescinda da interventi emergenziali, a tratti confusi e sovrapposti[59], rappresenterebbe senza dubbio il primo importante segnale di un cambio non solo di passo ma anche di strada. Una tale riflessione dovrebbe muovere dalla comprensione piena della delicatezza e complessità del corretto contemperamento tra libertà e potere, diritti fondamentali e tutela della sicurezza dinnanzi al proliferare di strumenti di sorveglianza massiva quali da conservazione generalizzata; del resto, come già evidenziato dall'Avvocato Generale Campos-Sánchez Bordona nelle Conclusioni riferite alla causa *La Quadrature du Net*, la garanzia delle esigenze securitarie deve trovare un confine chiaro nelle necessità di «assoggettamento del potere e della forza ai limiti del diritto e, in particolare, a un

[55] R. Flor - S. Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico*, cit., 53.

[56] Come rilevato da gran parte della dottrina, tra cui si ricordano L. Lupária, *Data retention e processo penale*, cit.; L. Scaffardi, *La data retention va in ascensore*, cit.; R. Flor - S. Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico*, cit.

[57] Sotto questo profilo, interessanti sono le considerazioni di A. Malacarne, *commento a prima lettura del DL 132/21 in materia di tabulati telefonici*, in *Sistema Penale*, 8 ottobre 2021.

[58] Oltre ai moniti già richiamati, mossi dal Garante per la Protezione dei Dati Pasquale Stanzione nel documento *Segnalazione sulla disciplina della conservazione* (cit.), anche il già Garante, Antonello Soro, non aveva mancato di esprimere perplessità e preoccupazioni quanto alla disciplina italiana in materia di *data retention*, sin dalla discussa adozione della Legge Europea 2017 (sul punto si leggano le dichiarazioni di Soro durante il Convegno *Privacy digitale e protezione dei dati personali tra persona e mercato*, reperibili sul sito web del Garante, nonché il Parere 8005333/2018).

[59] Taluni studiosi definiscono infatti la disciplina italiana in materia di *data retention* come frutto di una «tormentata stratificazione» (E. Andolina, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, cit.).

ordinamento giuridico che trova nella difesa dei diritti fondamentali la ragione e il fine della sua esistenza»; se così non fosse «nulla potrebbe assicurare che, dotando il potere pubblico di strumenti esorbitanti per il perseguimento dei reati (..) la sua azione incontrollata e totalmente libera non si risolverebbe in definitiva in un pregiudizio alla libertà di tutti», § 135[60].

Venendo infine al secondo ambito di approfondimento, le Conclusioni e la prossima decisione della CGUE nel caso qui analizzato rappresentano una ulteriore importante tappa di quel viaggio che, nella dimensione sovranazionale e nazionale, continua ad essere costellato di mete intermedie ma che pare essere, ancora oggi, privo di un punto di arrivo chiaro e definitivo. Il rinvio del giudice italiano, infatti, si inserisce in un percorso ancora in evoluzione, rispetto al quale diversi protagonisti stanno ancora concorrendo a determinarne la direzione e – forse – il traguardo finale.

Innanzitutto, non si può che mettere in luce come, nell'attuale immobilismo del legislatore europeo e nella spesso diversa interpretazione e posizione assunta da governi e Parlamenti nazionali quanto alla disciplina della *data retention*, i giudici di Lussemburgo siano nel frattempo chiamati a pronunciarsi in un altro rilevante rinvio promosso questa volta dal Consiglio di Stato francese. Il caso *La Quadrature du Net et al. c. Premier Ministre, Ministère de la Culture*, C-470/12, recentemente riassegnato alla Grande Sezione, è infatti osservato con grande attenzione e le Conclusioni dell'Avvocato Generale Szpunar del 27 ottobre 2022 hanno già iniziato a far discutere. Tale rinvio ha ad oggetto, nel limitato e specifico ambito della lotta alle violazioni dei diritti di proprietà intellettuale commesse online, la disciplina della *data retention* e accesso agli indirizzi IP attribuiti all'origine di una connessione Internet. La questione, che qui si vuole solo brevemente richiamare, prende avvio dalla normativa francese – il Decreto del 5 marzo 2010 – che consente la conservazione generalizzata, l'acquisizione e il trattamento – da parte di una particolare autorità – dei dati di connessione a scopi di lotta ai reati lesivi del diritto d'autore; questa disposizione, tuttavia, non prevede il controllo preventivo di un giudice o di un'autorità indipendente.

Nelle sue Conclusioni, l'Avvocato Generale Szpunar pare proporre un ripensamento della giurisprudenza della CGUE relativamente all'interpretazione dell'art. 15 Direttiva *e-Privacy* e, per quanto qui ci interessa maggiormente, muove considerazioni di rilievo anche sulla nozione di "forma grave di criminalità": questa deve «essere interpretata autonomamente. Essa non può dipendere dalle concezioni di ciascuno Stato membro, salvo permettere un'elusione dei requisiti di cui all'art. 15, par. 1, della direttiva 2002/58/CE a seconda che gli Stati membri adottino una concezione estensiva o meno della lotta alle forme gravi di criminalità», § 74. Una lettura, questa, che trova evidenti profili di contrapposizione con le Conclusioni dell'Avvocato Generale Collins nel caso sin qui esaminato, che giungono, sul punto, a negare il carattere di nozione autonoma di diritto dell'UE al concetto di "reato grave".

L'Avvocato Generale Szpunar, poi, seppure a condizioni ben determinate e unicamente con riferimento ai dati relativi all'identità civile corrispondenti ad indirizzi IP, rilancia una lettura del diritto dell'UE volta a consentire una conservazione generalizzata e un accesso non vincolato al controllo preventivo di un giudice o di una entità amministrativa indipendente; ciò però solo qualora lo scopo perseguito sia quello di permettere l'intervento e l'indagine da parte dell'autorità amministrativa incaricata di proteggere i diritti d'autore su Internet e unicamente nel caso in cui tali dati rappresentino il solo strumento di indagine in grado di consentire l'identificazione della persona alla quale l'indirizzo era attribuito al momento della commissione del reato.

Rispetto alla lettura qui sinteticamente riportata delle Conclusioni nel caso C-470/12,

[60] Si fa riferimento alle Conclusioni dell'Avvocato Generale Campos-Sánchez Bordona nel caso *La Quadrature du Net*, § 135.

alcune critiche e perplessità sono già state sollevate[61], rilevando nelle posizioni espresse dall'Avvocato Generale Szpunar i segni di un preoccupante *revirement* rispetto alla previa giurisprudenza della CGUE e di una interpretazione del diritto dell'UE maggiormente pro-securitaria, col rischio di "annacquare" e via via restringere i requisiti e i principi indicati dalla *case law* eurounitaria. Le visioni discordanti e le critiche, in direzioni differenti, già emerse a seguito della apertura a forme di *bulk data retention* per scopi di garanzia della sicurezza nazionale, sembrano quindi destinate a riproporsi nel prossimo futuro.

Le decisioni dei giudici di Lussemburgo in quest'ultimo caso – senza dubbio molto particolare e circoscritto quanto alla natura dei dati e dei reati perseguiti – e in quello esaminato nel presente lavoro determineranno l'evoluzione del dibattito europeo in materia non solo di *data retention* ma anche, più ampiamente, di tutela dei diritti fondamentali dinnanzi all'emergere di sempre più sofisticate tecniche di sorveglianza massiva e raccolta di dati. Il vivace e mai sopito confronto – e scontro – tra torsioni regolatorie securitarie e approcci maggiormente garantisti di diritti e libertà trova infatti ormai sempre nuova concretizzazione: si pensi al ricorso a sistemi innovativi di c.d. *predictive policing*, fondati su decisioni automatizzate, o ancora a strumenti massivi di riconoscimento facciale[62], che già hanno iniziato a mettere alla prova legislatori e corti, anche nell'UE[63], testimoniando così come la nota e antica contrapposizione – o

[61] In questo senso si è espressa la ONG EDRi (*Advocate General recklessly calls for watering down privacy protections*, 16 novembre 2022). In particolare, gli attivisti criticano la posizione dell'Avvocato Generale che ritiene i dati relativi agli indirizzi IP come meno invasivi della sfera privata e non in grado di consentire una ricostruzione della vita e delle preferenze degli utenti: «*in doing so, the AG plays down the level of privacy intrusion that identifying the person who has viewed certain online files may entail. Files including photos, videos or text are susceptible to reveal the person's sexual orientation, political, religious or philosophical opinion. There is no need to reconstruct the entire clickstream of the user in order to deduce very intimate information on their life*».

[62] Entrambi i sistemi di *predictive policing* e di riconoscimento facciale sono basati sull'impiego di strumenti di Intelligenza artificiale e sono impiegati – anche ma non solo – da *law enforcement authorities* o agenzie di *intelligence* al fine di anticipare la soglia del pericolo e svolgere analisi predittive di dati o immagini. Su questi strumenti innovativi – peraltro oggetto di attenzione anche nel dibattito normativo sovranazionale con riferimento alla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza artificiale –, si legga, *ex multis*, B. Perego, *Predictive policing: trasparenza degli algoritmi, impatto sulla privacy e risvolti discriminatori*, in *BioLaw Journal*, 2, 2020, 447 ss.; G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021; F. Paolucci, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in questa *Rivista*, 1, 2021, 204 ss.; E. Carpanelli, *Il ricorso all'Intelligenza artificiale nel contesto di attività di law enforcement e di operazioni militari: brevi riflessioni nella prospettiva del diritto internazionale*, in *DPCE Online*, 1, 2022, 383 ss.; M. Lo Monaco - J. Scipione, *Anatomia legale del riconoscimento facciale*, in *Fondazione Leonardo. Civiltà delle macchine*, 16 marzo 2022; S. Lonati, *Predictive policing: dal disincanto all'urgenza di un ripensamento*, in questa *Rivista*, 2, 2022, 302 ss.

[63] In materia di riconoscimento facciale, di grande rilievo è certamente la pronuncia dei giudici inglesi della Court of Appeal, Civil Division, 11 agosto 2020, *R(OTAO) Bridges v. The Chief Constable of South Wales Police and Others*, EWCA Civ 1058,; ma pensiamo anche al dibattito italiano, che ha visto l'intervento del Garante per la Protezione dei Dati con riferimento al sistema SariReal Time e Clearview AI e che ha conosciuto con d.l. 51/2023 l'approvazione di una proroga legislativa della moratoria sui sistemi di riconoscimento facciale in luoghi pubblici o aperti al pubblico estesa sino al 31 dicembre 2025 (già determinata dall'art. 9, c. 9, del d.l. 139/2021, convertito dalla l. 205/2021). In tema di *predictive policing*, di particolare interesse è la recente sentenza del Tribunale costituzionale federale tedesco del 16 febbraio 2023 che ha dichiarato l'incostituzionalità delle normative adottate dai Land di Hesse e Hamburg riguardanti l'implementazione di "automated data analysis for the prevention of criminal acts" (si rinvia sul punto alla Press Release No. 18/2023 del *Bundesverfassunsgericht* tedesco); anche la CGUE è attualmente chiamata a pronunciarsi su sistemi di *automated decision-making* fondati su strumenti di Intelligenza artificiale, nel caso C-634/21 (su tale caso e sullo stato di avanzamento del processo: A. Hauselmann, *The ECJ's first landmark case on automated decision-making. A Report from the oral hearing before the First Chamber*, in *European Law Blog*, 20 febbraio 2023).

rapporto – tra sicurezza e diritti fondamentali sia continuamente rinnovata dinnanzi al progresso tecnologico[64].

Ebbene, in tale ottica generale, il futuro di sistemi di sorveglianza massiva, tra cui la *data retention*, nell'UE e, in particolar modo, in Italia risulta ancora difficile da stabilire, soprattutto con riferimento a specifici e diversi profili regolatori, quali il ruolo delle autorità giurisdizionali nel controllo preventivo o il diverso vaglio di proporzionalità da svolgere in considerazione di finalità e tipologia di dati conservati[65]. Come si è avuto modo di vedere dall'analisi del caso in esame, molti sono gli interrogativi interpretativi da risolvere, concernenti soprattutto un vaglio di proporzionalità[66] divenuto sempre più centrale ma altrettanto complesso da determinare dinnanzi a posizioni spesso divergenti[67].

Attraverso i prossimi interventi giurisprudenziali, a livello nazionale e sovranazionale, nonché mediante le scelte normative interne o europee, le corti e i legislatori dovranno assumere il difficile ma improrogabile compito di identificare la meta finale di un percorso ancora in divenire e a tratti incerto; con un monito che dovrebbe muovere le decisioni – anche legislative – in tale complessa materia e che aiuta a comprendere la grande delicatezza della posta in gioco: «*it is to be hoped that the Court [la CGUE in questo caso] will succeed in disregarding the polarisation trap and fostering the adoption and development of new technologies that are compliant with fundamental rights*»[68].

[64] Il progredire delle tecnologie e l'affermarsi della società algoritmica, infatti, risultano in grado sì di ampliare potenzialità di controllo e prevenzione in ambito securitario, ma anche di incrementare rischi e minacce alle libertà su cui le nostre società democratiche e lo Stato di diritto si fondano. Per riflessioni approfondite sul tema, si veda, tra i molti, G. De Minico - O. Pollicino (eds.), *Virtual freedoms, terrorism and the law*, Torino-Londra, 2020; H-W. Micklitz - O. Pollicino - A. Reichman - A. Simoncini (eds.), *Constitutional challenges in the algorithmic society*, Oxford, 2021; G. De Gregorio, *Digital constitutionalism in Europe. Reframing rights and powers in the algorithmic society*, Cambridge, 2022; M. Ienca - O. Pollicino - L. Liguori - E. Stefanini - R. Andorno (eds.), *The Cambridge handbook of information, technology, life sciences and human rights*, Cambridge, 2022; E. Celeste, *Digital constitutionalism. The role of Internet Bills of Rights*, Londra, 2022.

[65] Come affermato da Albers, del resto, «*Retention of data generated in telecommunications in order to enable security agencies at a later point in time to gain access to and make use of this data for security purposes is an illustrative example of how the Internet impacts the forms surveillance takes and creates new challenges for fundamental rights*», M. Albers, *Surveillance and Data Protection Rights: Data Retention and Access to Telecommunications Data*, in M. Albers - I.W. Sarlet (eds.), *Personality and data protection rights on the Internet*, Cham, 2022, 69.

[66] De Vergottini evidenzia la necessità di respingere l'idea di un bilanciamento tra sicurezza e diritti fondamentali «perché il bilanciamento presuppone equivalenza di posizioni di partenza. Piuttosto, tenendo ferma la precedenza per i diritti si ammette in casi particolarmente gravi e meritevoli di ottenere una limitazione dei diritti ma a condizione che l'intervento limitativo sia giustificato e soprattutto proporzionato al fine che si deve conseguire con la misura», G. de Vergottini, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in *Rivista AIC*, 4, 2019, 85.

[67] Ciò emerge con tutta chiarezza dal dibattito normativo in corso sulla proposta di regolamento *e-Privacy*, già richiamato.

[68] V. Mitsilegas et al., *Data retention and the future of large-scale surveillance*, cit., 36.

Magistrati e social media: una riflessione alla luce dell'esperienza statunitense*

Silvio Roberto Vinceti

Abstract

Nel momento in cui plurimi segnali istituzionali adombrano l'opportunità di un intervento normativo sull'utilizzo dei social media da parte dei magistrati in Italia, appare di evidente importanza l'analisi delle esperienze di regolamentazione nel diritto comparato. Distinguendo tra gli approcci più restrittivi o più aperturisti adottati nei diversi Stati degli Stati Uniti d'America — che per diverse ragioni costituiscono la disciplina giuridica più risalente e articolata del fenomeno — lo studio enuclea innanzitutto i nodi giuridici fondamentali posti dall'utilizzo dei social media da parte dei magistrati. Vengono poi giustapposte due differenti impostazioni della questione di politica del diritto, che a loro volta accedono a diverse ricostruzioni degli interessi costituzionali rilevanti e, mediatamente, ad alternative concezioni del ruolo della magistratura nello Stato costituzionale di diritto.

With converging indications portending a policy intervention on the use of social media by judges in Italy, a review of foreign experiences appears of evident importance to the enactment of an overall convincing regulation on the subject. By distinguishing between the more restrictive and liberal approaches adopted in the United States — which, for different reasons, constitute the prime regulatory framework in the comparative landscape — the study outlines the key legal issues in the judges' use of social media. Furthermore, the essay articulates a reflection on two competing accounts of the constitutional interests bearing on the policy question, which in turn foreshadow contrasting understandings of the role of judges in contemporary constitutional democracies.

Sommario

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

Keywords

responsabilità disciplinare – magistrati – social media – diritto statunitense – ordinamenti giudiziari comparati

1. Introduzione

Molteplici ragioni inducono a pensare che la regolamentazione dell'utilizzo dei social media da parte dei "magistrati"[1] sia destinata a porsi come tema ineludibile nell'agenda normativa del legislatore italiano. Innanzitutto, esiste il dato dei diversi attori istituzionali che già hanno adombrato l'opportunità di un confronto con il fenomeno: agli ammonimenti del Presidente della Repubblica su di un uso prudente dei social media all'inaugurazione dei corsi della Scuola Superiore della Magistratura nell'aprile del 2019[2] hanno fatto seguito una apposita Delibera del Consiglio di Presidenza della

[1] Seguendo l'esempio di autorevole dottrina (v. ad es. L. Montanari, *L'indipendenza della magistratura in Europa. Verso un modello comune di garanzie?*, in R. Toniatti - M. Magrassi (a cura di), *Magistratura, giurisdizione ed equilibri istituzionali. Dinamiche e confronti europei e comparati*, Padova, 2011, 104, nota 2) si accompagna l'impiego dei termini "magistrati" e "magistratura" all'espresso *caveat* che il termine di comparazione qui preso in considerazione è la sola autorità giudicante dell'ordinamento straniero — in questo caso, i giudici statunitensi — con esclusione, dunque, della corrispondente autorità requirente. Stante infatti il più accentuato ruolo "di parte" e la corrispondente minor aspettativa sulla loro terzietà e imparzialità, ai *prosecutor* americani si applicano "soltanto" gli standard disciplinari previsti per gli avvocati e non quelli più stringenti previsti per i giudici. Questo non significa, beninteso, che l'utilizzo dei social media da parte dei *prosecutor* non susciti problemi disciplinari: v. ad es. K.K. Van Namen, *Facebook Facts and Twitter Tips—Prosecutors and Social Media. An Analysis of the Implications Associated with the Use of Social Media in the Prosecution Function*, in *Mississippi Law Journal*, 3, 2011, 568 ss. Anzi, secondo alcuni l'utilizzo dei social media «*exacerbates longstanding concerns regarding prosecutors' extrajudicial statements*»: «*The vast differences between traditional media and social media, including the way in which social media is far-reaching, unmediated, informal, and uniquely permanent, increase the likelihood that prosecutors' extrajudicial speech will harm the defendant, the fair administration of justice, and public perception of the legal profession. Thus, additional restraints are needed to restore the free speech/fair trial balance and promote professionalism in the social media age*» (E.A. Vance, *Should Prosecutors Blog, Post, or Tweet? The Need for New Restraints in Light of Social Media*, in *Fordham Law Review*, 1, 2015, 406). Che i social media apertamente mostrino la necessità di «*subject prosecutors to standards of conduct similar to those that apply to judges when that conduct may influence public perceptions of impartiality and integrity*» è stato di recente sostenuto da A.B. Long, *Of Prosecutors and Prejudice (or «Do Prosecutors Have an Ethical Obligation Not to Say Racist Stuff on Social Media?»)*, in *UC Davis Law Review*, 3, 2022, 1752–1754. In questo senso, la questione "social media" rinforza il già diffuso convincimento dottrinale sull'utilità di categorie disciplinari *ad hoc* per i *prosecutor* in quanto «ministers of justices»: v. ad es. B.A. Green, *Prosecutorial Ethics as Usual*, in *University of Illinois Law Review*, 5, 2003, 1604.

[2] Intervento del Presidente della Repubblica Sergio Mattarella alla cerimonia di inaugurazione dei corsi di formazione della Scuola Superiore della Magistratura per l'anno 2019. Questo il passaggio rilevante ai nostri fini: «In questa direzione, la Scuola organizza, ormai con una certa sistematicità, un corso su "L'etica professionale del magistrato". Si tratta di una attività formativa preziosa che sollecita il dibattito su temi sempre attuali, poiché comporta una riflessione sulle modalità attraverso le quali il ruolo e la funzione del magistrato, come delineati nella Costituzione, devono trovare concreta espressione nella

giustizia amministrativa[3], nonché alcune eloquenti risposte della Corte Suprema di Cassazione ad un questionario *in subiecta materia* della Corte Suprema della Repubblica Ceca[4]. Questa crescente consapevolezza nazionale rispetto al problema *de quo* si unisce ad una più risalente sensibilità da parte di organismi sovranazionali di cui l'Italia è membro[5]: anche in ragione dell'influsso di queste organizzazioni sull'ordinamento giuridico domestico, è difficile pensare che una "competente istituzione normativa"[6]

società. Vorrei sottolineare come, in questo ambito, una nuova questione, delle più delicate, è quella che riguarda l'uso dei social media da parte dei magistrati: si tratta di strumenti che, se non amministrati con prudenza e discrezione, possono vulnerare il riserbo che deve contraddistinguere l'azione dei magistrati, e potrebbero offuscare la credibilità e il prestigio della funzione giudiziaria». Sul discorso presidenziale v. L. Longhi, *I magistrati e l'uso dei* social. *Appunti sulla deontologia professionale di categoria nell'era della comunicazione di massa*, in *Dir. pubb. eur. rass. online*, 1, 2019, 192 ss., 199, che richiama l'opportunità di discutere il problema nel contesto della più ampia riflessione intorno alla «legittimazione democratica della giurisdizione» (ivi, 197).

[3] *Delibera sull'uso dei mezzi di comunicazione elettronica e dei* social media *da parte dei magistrati amministrativi* (all. 1 verbale 18 marzo 2021, n. 11) [da qui *Delibera CGA*] su cui v. diffusamente A. Lollo, *Libertà di manifestazione del pensiero e uso dei social da parte dei magistrati*, in *Consulta Online*, 3, 2022, 1068–1073. Istruita alle risultanze della documentistica internazionale, la Delibera si mostra particolarmente consapevole dei rischi e delle necessità regolative del fenomeno "social media" e in questo senso deve pienamente sottoscriversi il giudizio per cui «[a]ncora una volta [...] la giustizia amministrativa si rivela pioniera nell'uso delle tecnologie informatiche» (ivi, 1069). Più che i generali limiti del sistema disciplinare della magistratura amministrativa (su cui v. cfr. P. Mantini, *Profili critici e di riforma della responsabilità disciplinare della magistratura amministrativa*, in *federalismi.it*, 20, 2017, 2 ss., spec. 23–46, nonché la tavola rotonda in G. Campanelli (a cura di), *Indipendenza, imparzialità e responsabilità dei giudici speciali*, Pisa, 2013, 151 ss.) pesano sulla capacità normativa della Delibera i dubbi sulla natura giuridica dell'atto, da ritenersi con ogni probabilità espressione di *soft law* (A. Lollo, *Libertà di manifestazione del pensiero e uso dei social da parte dei magistrati,* cit., 1074).

[4] *Risposte della Corte Suprema di Cassazione al questionario proveniente dalla Corte Suprema della Repubblica Ceca su "Le attività secondarie e l'uso dei social media da parte dei magistrati"*, elaborate grazie all'apporto scientifico dell'Ufficio del Massimario (redattore dott. Paolo Spaziani), 30 settembre 2021.

[5] Si v., da ultimo, l'adozione da parte del Consiglio consultivo dei giudici europei (CGUE) dell'*Opinion 2 dicembre 2022, n. 25, sulla libertà di espressione dei magistrati,* da qui *CGUE Opinion 25/2022*, il cui ottavo capitolo è dedicato all'utilizzo dei social media da parte dei giudici. L'*Opinion* si giova peraltro della lunga discussione sui limiti alla libertà di espressione dei magistrati nella giurisprudenza della Corte europea dei diritti dell'uomo: al riguardo, con specifico riferimento al tema dei social media, si v. J. Jahn, *Social Media Communication by Judges. Assessing Guidelines and New Challenges for Free Speech and Judicial Duties in the Light of the Convention*, in M. Elósegui - A. Miron - I. Motoc (a cura di), *The Rule of Law in Europe. Recent Challenges and Judicial Responses*, Cham, 2021, 137 ss., nonché A. Seibert-Fohr, *Judges' Freedom of Expression and Their Independence. An Ambivalent Relationship*, in M. Elósegui - A. Miron - I. Motoc (a cura di), *The Rule of Law in Europe. Recent Challenges and Judicial Responses*, Cham, 2021, 89 ss. Si confronti inoltre il lavoro svolto dal *Global Judicial Integrity Network* dell'Ufficio delle Nazioni Unite sulla Droga e il Crimine (UNODC), di cui un primo risultato sono le *Linee guida non vincolanti sull'utilizzo dei social media da parte dei giudici* del 2019 (trad it. Daniela Cavallini, Francesco Contini e Andrea Zanzottera) [da qui *Linee Guida UNODC*], su cui v. il commento di S. Sica, *Social media e magistratura*, in *Tecn. dir.*, 2, 2020, 562–564. Si v. altresì i *report* prodotti dalla Rete europea dei Consigli di Giustizia, tra cui spiccano il *Report on Justice, Society and the Media* del 2012 e l'*ENCJ report on Public Confidence and the Image of Justice* del 2019, su cui v. E. Bruti Liberati, *Delitti in prima pagina. La giustizia nella società dell'informazione*, Milano, 2022, 197–198.

[6] La formula "compente istituzione normativa" è tanto volta ad accantonare, ai fini della presenta ricerca, l'annosa controversia sui limiti normativi della potestà organizzativa del Consiglio superiore della magistratura quanto ad includere la competenza regolatorio-deontologica dell'Associazione nazionale magistrati (ANM). Rispetto a quest'ultimo profilo, è suggestivo notare come l'adozione del nuovo Codice etico dell'ANM nel 2010 sia stata occasionata anche dalla necessità di prendere «posizione sul delicato versante dei rapporti col mondo dell'informazione e soprattutto con le degenerazioni delle comunicazioni di massa»: da questa ispirazione è discesa la previsione di cui all'art. 6, ove si afferma, tra l'altro, che «[f]ermo il principio di piena libertà di manifestazione del pensiero, il magistrato si ispira a

italiana non sarà presto chiamata ad assumere una posizione più organica sull'utilizzo dei social media da parte dei magistrati.

Insieme alla crescente avvertenza istituzionale rafforzano l'opportunità di un intervento normativo alcuni elementi specifici del tema considerato e del contesto giuridico italiano. Da una parte, nonostante in alcuni ordinamenti comparati parrebbe astrattamente possibile applicare ai social media già vigenti fattispecie disciplinari "ad ampio respiro" — come è il caso, appunto, degli Stati Uniti d'America — pure qui si fatica a sfuggire alla sensazione che il fenomeno "social media" rappresenti una sfida del tutto inedita, irriducibile a quelle poste dai tradizionali mezzi di comunicazione di massa e per cui le vigenti categorie della responsabilità del magistrato possono risultare inefficaci[7]. Da altra parte, la verosimile opportunità di un intervento normativo *ad hoc* è giustificata dal peculiare contesto dell'ordinamento giudiziario italiano, che con la scelta di una tipizzazione "in senso forte" rende in ipotesi necessario un intervento aggiuntivo da parte del legislatore per far fronte a "nuove" situazioni disciplinari[8], come alcuni note vicende hanno problematicamente ricordato[9].

Rispetto ad altri contributi sul tema, il presente saggio intende fornire un ulteriore tassello ai fini della risoluzione del "puzzle normativo" rappresentato dall'utilizzo dei social media da parte dei magistrati mediante il vaglio della regolamentazione e della discussione del fenomeno nel diritto statunitense. Mentre l'idea di un approccio comparatistico alle sfide dell'ordinamento giudiziario italiano è operazione tanto risalen-

criteri di equilibrio, dignità e misura nel rilasciare dichiarazioni ed interviste ai giornali e agli altri mezzi di comunicazione di massa, così come in ogni scritto e in ogni dichiarazione destinati alla diffusione». Benché qui il riferimento fosse ai mass media tradizionali, il riferimento all'«equilibrio, dignità e misura» è stata ripreso in un emendamento non approvato del 2018 («Il magistrato utilizza i social network e gli altri strumenti di comunicazione telematica consapevole del proprio ruolo professionale, astenendosi da comportamenti che possono ledere la credibilità della funzione giudiziaria e della magistratura nel suo complesso») come criticamente rilevato da E. Bruti Liberati, *Un punto di arrivo o un punto di partenza?*, in *Quest. giust.*, 4, 2018, 320, secondo cui, diversamente dal passato, l'ANM non si sarebbe mostrata, qui, «attenta a cogliere i fatti nuovi ed in particolare le derive della "giustizia mediatica"».

[7] V. *infra* § 2.4.

[8] Dovendosi verificare, in concreto, il margine di trattabilità del nuovo *medium* secondo le categorie previste dagli artt. 2, 3, 4, del d.lgs. 23 febbraio 2006, n. 109. Una prima significativa analisi di questo tipo è stata condotta da S. Sica, *Social media e magistratura*, cit., 552–555, che ha rimarcato il ruolo dell'interprete nell'adeguamento delle disposizioni disciplinari vigenti: «In altre parole, il quesito è: occorrono nuove norme specifiche sull'argomento in esame, a modifica dell'impianto disciplinare della magistratura? Si può forse serenamente rispondere no; d'altronde, per esempio, i civilisti più accorti sanno che la disciplina codicistica del contratto può trovare pacifica applicazione anche al contratto telematico; sta all'interprete del caso concreto compiere lo sforzo di adeguamento tra la norma e lo *specificum* del *medium* di conclusione del contratto» (ivi, 565). Rimane tuttavia possibile chiedersi quali margini di operabilità possa avere qui un'interpretazione analogica *in malam partem*, stante la natura giurisdizionale — pur controversa (*ex plurimis* G. Campanelli, *Il giudizio disciplinare dei magistrati ordinari. Procedimento o processo? Natura, garanzie, criticità e ipotesi di riforma*, Torino, 2018, 86–91) — e la finalità afflittiva del procedimento disciplinare. In tema, seppur nel contesto di un'analisi sul più ampio *genus* del pubblico impiego, altresì C. E. Guarnaccia, *La prima giurisprudenza sul rapporto tra pubblico impiego e social media*, in *Inf. dir.*, 1–2, 2017, 375–376.

[9] Il riferimento è alla "vicenda Palamara" e alla decisione della Procura generale della Corte di Cassazione di escludere il rilievo disciplinare della mera «attività di autopromozione» del magistrato con la controversa Direttiva 22 giugno 2020 (n. 493/20/SD2), su cui v. criticamente R. Russo, *Riflessione su procedimenti disciplinari e archiviazioni*, in *La Magistratura*, 2022.

te[10] quanto attuale[11] — nonché foriera di recentissime introduzioni legislative[12] — da far apparire forse ingiustificate lunghe premesse d'indagine, più cogente diviene, in sede di introduzione, l'esplicazione delle ragioni che hanno portato all'individuazione dell'ordinamento statunitense come termine di paragone straniero. Per il vero, la scelta è risultata l'esito, più che il punto di partenza, dell'indagine di diritto comparato: benché infatti il problema dell'utilizzo dei social media da parte dei magistrati interessi tutti gli ordinamenti costituzionali contemporanei[13] e abbia trovato prime significative regolamentazioni negli ordinamenti giudiziari di Francia[14], Inghilterra-Galles[15] e Brasile[16], lo studioso è costretto a constatare una evidente sproporzione tra l'attenzione riservata al tema nel diritto e nella dottrina statunitensi e la trattazione nelle altre giurisdizioni nazionali, sia dal punto di vista del diritto positivo che della ricerca scientifica. La prominenza dell'esperienza, riconosciuta peraltro nella documentistica internazio-

[10] Sul tema v. da ultimo M. Volpi, *L'ordinamento giudiziario nella prospettiva comparata*, in G. Ferri - A. Tedoldi (a cura di), *L'ordinamento giudiziario a dieci anni dalla legge n. 150 del 2005*, Napoli, 2016, 96–98.

[11] V. ad es. le riflessioni collezionate in *DPCE Online*, n. 4/2020, sul tema del governo autonomo della magistratura, con contributi di Volpi, Ferri, Montanari, Iacometti, Costantini, Aravantinou Leonidi, Penasa, Lubello, Mazza, Delledonne, Bertolini, Marchetti e Tarchi, Torre, Ceccherini, Bussi, Catani, Duranti, Paffarini.

[12] Si pensi, ad es., all'istituto dell'ufficio del processo (UPP) ed in particolare alla figura degli Addetti UPP di cui all'art. 11 d.l. 9 giugno 2021, n. 80, rispetto ai quali lo stesso Ministero della Giustizia ha esplicitato, nelle *slide* di accompagnamento, l'ispirazione comparata ai *law clerck* anglosassoni, agli *assistant de justice* francesi nonché all'*oficina judicial* spagnola. Cfr. *L'Ufficio per il processo e l'investimento sul capitale umano* (luglio 2021).

[13] Salvo quanto si dirà nelle successive note su Francia, Regno Unito e Brasile, si segnalano gli ulteriori studi compulsati afferenti ad altri ordinamenti: per il Canada L. Sossin - M. Bacal, *Judicial Ethics in a Digital Age*, in *U.B.C. Law Review*, 3, 2013, 629 ss.; per l'Australia J. Gibson, *Social Media and the Electronic New World of Judges Professional*, in *International Journal for Court Administration*, 2, 2016, 1 ss.; sulla Germania la discussione nella monografia di J. Jahn, *Die Medienöffentlichkeit der Rechtsprechung und ihre Grenzen*, Baden-Baden, 2021, 381 ss.; sulla Spagna C.C.M. Montero, *La comisión ética judicial y la libertad de expresión*, in E. García-Cuevas Roque (a cura di), *Ética del jurista y ética social*, Madrid, 2022, 77 ss., e A. Casadevall Portas, *Jueces y redes sociales*, Vila Nova de Gaia, 2023. Sul Gana v. K.K. Adu, *The use of social media by African judges. The Ghanaian experience*, in *Information Development*, 1, 2022, 40 ss.

[14] In Francia, la *Charte de déontologie de la juridiction administrative* è stata emendata nel 2018 appositamente per «*prend en compte le développement exponentiel des réseaux sociaux*» (ivi, 10). La seconda edizione della *Recueil des obligations déontologiques des magistrats*, Paris, 2019, contiene inoltre plurimi riferimenti al tema (ivi, part. 71–81): v. al riguardo, S. Sica, *Social media e magistratura*, cit., 558, e E. Bruti Liberati, *Delitti*, cit., 199–200.

[15] Nell'ordinamento giudiziario dell'Inghilterra-Galles, la *Guide to Judicial Conduct* è stata modificata nel marzo del 2018 per affrontare, tra l'altro, «the rise of social media» (ivi, 3). Il documento — che può essere considerato una guida orientativa paranormativa — riprende peraltro concetti già espressi nella raccomandazione *Blogging by Judicial Office Holders* adottata nel 2012 per conto del *Senior Presiding Judge* e del *Senior President of Tribunals*. S. Sica, *Social media e magistratura*, cit., 559–560.

[16] In Brasile, un provvedimento del *Corregedor Nacional de Justiça* 13 giugno 2018, n. 71 (*Dispõe sobre o uso do e-mail institucional pelos membros e servidores do Poder Judiciário e sobre a manifestação nas redes sociais*) e una successiva risoluzione 17 dicembre 2019, n. 305, adottata dal *Presidente do Conselho Nacional De Justiça* (*Estabelece os parâmetros para o uso das redes sociais pelos membros do Poder Judiciário*) hanno sancito l'adozione di un approccio restrittivo rispetto all'utilizzo dei social media da parte di magistrati. Le associazioni professionali hanno tuttavia reagito impugnando gli atti per violazione della libertà di espressione: due azioni cautelari intentate contro il provvedimento n. 71/2018 sono state rigettate, mentre contro la risoluzione n. 305/2019 sono state proposte due azioni dirette di incostituzionalità e un ricorso di sicurtà.

nale[17], impone in questo senso una trattazione specifica.
Dal punto di vista della progressione argomentativa dell'indagine, dopo qualche breve elucubrazione sulle ragioni di una così accesa attenzione al tema (§ 2.1) e alcuni cenni introduttivi sulla responsabilità del giudice nel diritto statunitense (§ 2.2) si discuteranno la regolamentazione del fenomeno nel diritto positivo (§ 2.3.1) e i nodi fondamentali attorno a cui è ruotata la riflessione dottrinale (§ 2.3.2). Alla discussione di più stretto diritto straniero segue poi il momento di comparazione con l'ordinamento italiano (§ 3). Qui, più che l'avanzamento di una specifica posizione *de iure condendo*, si è inteso concentrarsi su una linea di riflessione che dovrebbero apparire rilevante qualsiasi posizione, più o meno restrittiva, sia presa in considerazione dal legislatore di riforma: la definizione dei valori costituzionali che possono entrare nella valutazione comparativa degli interessi (§ 3.1). Giustapponendo la tradizionale contrapposizione degli interessi nella materia *de qua* — quella tra libertà di manifestazione del pensiero del magistrato e interesse all'imparzialità nell'amministrazione delle giustizia — ad alcuni "ulteriori interessi" a cui è stata funzionalizzata la partecipazione del magistrati ai social media nella riflessione statunitense, si sostiene che la scelta tra le due modalità di inquadramento della problematica — e dunque l'inclusione di questi "ulteriori interessi" nella valutazione comparativa — dipenda in larga misura dalla diversa concezione del ruolo del potere giudiziario nello Stato costituzionale di diritto (§ 3.1.3).

2. Giudici e social media: l'esperienza americana

2.1. Le ragioni di una speciale attenzione

In nessun ordinamento il tema dell'utilizzo dei social media da parte dei magistrati — nonché, per il vero, di altri operatori giuridici[18] — è stato scandagliato e dibattuto

[17] V. più diffusamente su questo punto *infra* § 2.1.

[18] Ad es., membri della giuria e avvocati su cui v. P. Sammarco, *Giustizia e social media*, Bologna, 2019, 145 ss. Altro problema specifico è l'utilizzo dei social media da parte di organi *lato sensu* servienti all'esercizio della funzione giurisdizionale come assistenti giudiziari, cancellieri, tirocinanti. Le obbligazioni disciplinari del giudice e quelle di queste altre categorie finiscono infatti per saldarsi nel momento in cui al magistrato è ascrivibile un generale obbligo di vigilanza sulle condotte degli altri partecipanti al processo: «*One key reason for requiring judges to be conversant in relevant technology has less to do with the judges themselves than with those appearing in their courtrooms, such as lawyers, courtroom staff, and even jurors. Maintaining courtroom decorum and protecting the integrity of the justice system is part of the judicial role. And while judges necessarily depend upon counsel appearing before them to help achieve these goals by reminding litigants and witnesses to adhere to the court's instructions, the fact remains that technology misuse can threaten the integrity of the system. From jurors tweeting or commenting online about the cases before them — such as "researching" the parties and issues online — to lawyers failing to uphold their duty of candor to the tribunal, the sanctity of the trial process can be undermined by the online misconduct of those participating in the process. Judges must not only be aware of the potential for such misbehavior by those in their courtrooms; they should also have at least a basic grasp of the technology that could enable such undermining of the court's authority*» (J.G. Browning, *Should Judges Have a Duty of Tech Competence?*, in *St. Mary's Journal on Legal Malpractice and Ethics*, 2, 2020, 186–187). Sul tema anche J.G. Browning, *It's 3 A.M. Do You Know What Your Staff Just Posted? Social Media Ethics Pitfalls for Appellate Lawyers and Judges*, in *Journal of Appellate Practice and Process*, 1, 2022, spec. 60–64, 70–77). Sul diverso problema della responsabilità del giudice per i commenti lasciati da altri sulle pagine social del magistrato v. J.G. Browning, *Judged by the (Digital) Company You Keep. Maintaining Judicial Ethics in an Age of Likes, Shares, and Follows*, in *St. Mary's Journal on Legal Malpractice and Ethics*, 2, 2022, 230–237.

come negli Stati Uniti d'America. Il dato, del resto, è pacificamente riconosciuto in sede internazionale, come testimonia la frequenza delle esperienze statunitensi nei riferimenti e nelle citazioni dei documenti redatti dalle organizzazioni internazionali attive sull'argomento[19]. Conforta un simile giudizio che chi si è occupato dei generali problemi portati dall'avvento dei social media all'amministrazione della giustizia abbia fatto principale riferimento — per il tema *de quo* — proprio all'esperienza statunitense[20]. Questa speciale attenzione riservata al tema da parte dei legislatori e studiosi americani finisce tuttavia per destare la curiosità nello studioso e impone un accenno di spiegazione, se non altro al fine di verificare la tenuta di alcune risalente ipotesi sulla *species* del costituzionalismo americano. Al riguardo, sembra verosimile pensare che plurime ragioni concorrano a determinare l'acceso interesse per i problemi posti dall'utilizzo dei social media da parte dei magistrati nel diritto statunitense.

Una prima ragione di stretto diritto costituzionale può ritrovarsi nella naturale federale del sistema giudiziario statunitense. Come ampiamente noto, infatti, negli Stati Uniti la giustizia è "autonomamente" amministrata da cinquanta diverse realtà statali, un sistema di Corti locali per il Distretto di Columbia ed un apposito sistema giudiziario per l'ordinamento federale composto di quasi novecento membri[21]. Con una simile plura-

[19] Si vedano ad es. i riferimenti contenuti nel *discussion paper* del 2018 *Use of Social Media by Judges*, successivamente aggiornato dopo il confronto tra gli esperti nella versione *Discussion Guide. The Use of Social Media by Judges* del 2019. Entrambi i documenti sono stati prodotti dal *Global Judicial Integrity Network* ai fini della realizzazione delle già ricordate *Linee Guida UNODC*.

[20] P. Sammarco, *Giustizia e social media,* cit., 122, 132–145, V. Zeno-Zencovich, *Social Media and Fair Trial*, in R.L. Weaver - M.D. Cole - S.I. Friedland - D. Fairgrieve - A. Koltay - A. Raynouard (a cura di), *Free Speech, Privacy and Media. Comparative Perspectives*, vol. XI, Durham, 2020, 66, nota 5. Nello stesso senso v. il più ampio spazio dedicato all'esperienza statunitense in S. Sica, *Social media e magistratura*, cit., spec. 558–564. Il giudizio sulla centralità dell'esperienza statunitense in materia di giudici e social media appare del resto coerente con precedenti analisi sui mezzi di comunicazione di massa "tradizionali" e il più ampio fenomeno della «spettacolarizzazione della giustizia», di cui può considerarsi parte «una elevata "personalizzazione" della funzione giurisdizionale», con l'annessa «ricerca di protagonismo mediatico da parte di alcuni "signori del diritto", tra i quali gli avvocati e spesso anche gli stessi magistrati (specie se titolari di funzioni requirenti)» (G. Resta, *Il problema dei processi mediatici nella prospettiva del diritto comparato*, in Id. (a cura di), *Il rapporto tra giustizia e mass media. Quali regole per quali soggetti (Atti del Convegno di Bari, 4 luglio 2008)*, Napoli, 2010, 14, 18): già in quel frangente, infatti, si era osservato che «[i]l tema è letteralmente esploso nel contesto statunitense, ove l'interazione tra diversi fattori istituzionali — trai quali il ruolo attribuito alla giuria interamente laica, l'ampia discrezionalità del *prosecutor* e soprattutto la sostanziale insindacabilità dell'esercizio della libertà di stampa di cui al Primo Emendamento della Costituzione — ha creato una sorta di cortocircuito, il quale ha finito in diversi casi […] per "prendere in ostaggio" le garanzie previste dal Sesto Emendamento della Costituzione USA» (ivi, 13–14).

[21] Sull'ordinamento giudiziario americano, nella letteratura italiana, L. Mayers, *The American Legal System. The Administration of Justice in the United States by Judicial, Administrative, Military, and Arbitral Tribunals*, New York-Evanston-London, 1964; J.H. Merryman, *Judicial Responsibility in the United States*, in A. Giuliani - N. Picardi (a cura di), *L'educazione giuridica*, vol. III, Perugia, 1978, 263 ss.; M.C. Bassiouni, *The Judicial Sytem of The United States. An Overview*, in N. Picardi - A. Giuliani (a cura di), *L'ordinamento giudiziario*, vol. II, Rimini, 1983, 433 ss.; M.C. Bassiouni - S. Cunnigham, *Il sistema giudiziario*, in E. Amodio - M.C. Bassiouni (a cura di), *Il processo penale negli Stati Uniti d'America*, Milano, 1988, 3 ss.; A. Pizzorusso, *Sistemi giuridici comparati*, Milano, 1998, 228–231; L. Spadacini, *Separazione dei poteri e funzione giurisdizionale. L'esperienza nordamericana e il divergente approccio delle democrazie europee*, Brescia, 2012, 85 ss.; A. Gambaro - R. Sacco, *Sistemi giuridici comparati*, Milano, 2018, 140–141; A. Sperti, *Il potere giudiziario*, in G. D'Ignazio (a cura di), *Il sistema costituzionale degli Stati Uniti d'America*, Milano-Padova, 2020, 327 ss.; U. Mattei - E. Ariano, *Il modello di* common law, Torino, 2018, 119 ss.; V. Varano - V. Barsotti, *La tradizione giuridica occidentale. Testo e materiali per un confronto civil law common law*, Torino, 2021, 323 ss.; C. Bassu - M. Betzu - F. Clementi - G. Coinu, *Diritto costituzionale degli Stati Uniti d'America*, Torino, 2022, 75 ss.

lità di legislatori — spesso caratterizzati da divergenti sensibilità politiche — diviene in qualche modo fisiologica la proliferazione di approcci diversificati alla risoluzione dei problemi posti dall'amministrazione della giustizia: come è stato infatti ricordato proprio nel contesto del problema che ci occupa, in ragione del "federalismo giudiziario"[22] «*what may be permissible in one state or even in the majority of states may not be permissible in other states*»[23]. Rendendo immediata la comparazione tra i diversi approcci interni, il federalismo giudiziario non può che solleticare lo sviluppo della riflessione dottrinale. Nulla di più lontano, da questo punto di vista, dall'esperienza italiana, ove al contrario — e, beninteso, del tutto legittimamente — la giurisdizione è sempre stata vista come «baluardo della statualità unitaria»[24] e in forza di una «tradizione culturale profonda che tende ad identificare statualità e giurisdizione»[25] le forme di decentramento dell'organizzazione della giustizia si sono esaurite in modalità tutto sommato secondarie[26], ovvero di prospettica — e problematica — attuazione costituzionale[27].

In secondo luogo, è ragionevole pensare che contribuisca al fiorire della questione "magistrati e social media" un'altra nota sfaccettatura del costituzionalismo americano: la previsione, in plurime realtà statuali, di un reclutamento elettorale del personale magistratuale[28]. Nel momento in cui l'aspirante giudice deve vincere su altri candidati in una competizione elettorale — o se non altro essere confermato in una *retention election*[29] — l'utilizzo dei social media diventa uno strumento fondamentale, capace

---

[22] Definibile come l'idea di «*independence and interrelationship of federal and state courts*», C.P. Banks - D.M. O'Brien, *The Judicial Process. Law, Courts, and Judicial Politics*, II ed., St. Paul, 2021, 586. Da questo punto di vista, Stati Uniti e Germania sono spesso considerati i due «"modelli classici" di "federalismo giudiziario"», L. Montanari, *Il pluralismo normativo in Argentina e le sue ricadute sulla giurisdizione*, in *DPCE Online*, 1, 2020, 147). Benché connesso, diverso significato acquisisce la formula nella nozione di "*new judicial federalism*" con cui si è invece inteso descrivere l'idea per cui le corti statali «dovrebbero […] assumere un ruolo propulsivo, o di sperimentazione, nella tutela dei diritti individuali, essendo loro concesso superare, ma solo in senso maggiormente favorevole ai cittadini, le decisioni della Corte Suprema», M.E. Comba, *Esperienze federaliste tra garantismo e democrazia. Il «judicial federalism» negli Stati Uniti*, Napoli, 1996, 269. Altresì sul tema, di recente, A. Buratti, *Diritti fondamentali e integrazione federale. Origini, applicazioni e interpretazioni della due process clause nella Costituzione americana*, in *Diritti comparati*, 1, 2020, 42 ss.

[23] P.M. Reyes Jr., *To Post Or Not to Post. Judges on Social Media*, in *Judges' Journal*, 3, 2019, 21.

[24] E. Gianfrancesco, *Le Regioni italiane e la giurisdizione*, in *Teoria del diritto e dello Stato*, 1–2–3, 2006, 428.

[25] Ivi, 423.

[26] Cfr. la discussione delle Regioni a statuto speciale discussa in ivi, 404 ss.

[27] È il controverso tema — benché per certi versi negletto — delle «ulteriori forme e condizioni particolari di autonomia» nella materia «organizzazione della giustizia di pace», di cui all'art. 116, c. 3, Cost., su cui cfr. la diversa impostazione di S. Mangiameli, *Appunti a margine dell'art. 116, comma 3, della Costituzione*, in *Le Regioni*, 4, 2017, 671–672, e quella di M. Olivetti, *Il regionalismo differenziato alla prova dell'esame parlamentare*, in *federalismi.it*, 6, 2019, 12.

[28] «*One reason for the increased use of social media by judges may be the growing importance of these platforms in political races. With thirty-nine states using some form of election to select their trial judges, and thirty-nine states using some form of election to select their appellate court judges, use of social networking platforms as a political tool in the United States has become necessary to professional survival*» (J.G. Browning, *The Judge as Digital Citizen. Pros, Cons, and Ethical Limitations on Judicial Use of New Media*, in *Faulkner Law Review*, 1, 2016, 131–132).

[29] Sul reclutamento dei magistrati nell'ordinamento giudiziario statunitense v., nella dottrina italiana, S. Volterra, *L'indipendenza del giudice negli Stati degli Stati Uniti d'America*, Milano, 1970, 299 ss.; C. Punzi, *Il giudice onorario elettivo e l'attuazione dell'art. 106 della costituzione*, in *Riv. trim. dir. proc. civ.,* 1969, 273–275; J.H. Merryman, *Judicial Responsibility in the United States,* cit., 266–269; V. Vigoriti, *L'elezione del giudice*

di piegare a proprio favore il diffuso disinteresse che spesso circonda le elezioni dei giudici. In questo senso, si è affermato che i candidati «necessitano» di account Facebook, Twitter o Instagram se vogliono fare presa sulla base elettorale[30]: per usare una espressione efficace della riflessione dottrinale, sarebbe infatti «political malpractice» il mancato utilizzo dei social media da parte del candidato giudice[31].

Da ultimo, è facile pensare che le ragioni giuridico-costituzionali si saldino a fattori storico-culturali. Innanzitutto, internet e i social media sono — almeno cronologicamente — una ulteriore pagina dello sviluppo tecnologico americano[32] ed in questo senso appare comprensibile che i primi interessati alle ricadute giuridiche dell'avvento dei social media sull'amministrazione della giustizia siano proprio i legislatori e gli studiosi statunitensi. Alla peculiarità storica dell'oggetto "social media" fa da pendant la speciale considerazione di cui ha sempre goduto l'elemento soggettivo della nostra indagine: fin dalla celebre testimonianza di Tocqueville[33], conosciamo infatti la

nell'esperienza americana. Un'ipotesi di partecipazione popolare alla giustizia, in *Soc. dir.*, 1–2, 1979, 153 ss.; V. Vigoriti, *Le responsabilità del giudice. Norme, interpretazioni, riforme nell'esperienza italiana e comparativa*, Bologna, 1984, 23–31.

30 «*Judicial elections are usually last on the ballot and of minimal political interest to the average voter, so the massive outreach provided by ESM is essential for a candidate. Judicial candidates need a "Facebook" page to post campaign information and a "Twitter" or "Instagram" account to get their message out to the voter base in a resourceful manner*», M.S. Kurita, *Electronic Social Media. Friend or Foe for Judges*, in *St. Mary's Journal on Legal Malpractice and Ethics*, 2, 2017, 196. Altresì, E. Thornburg, *Twitter and the #So-CalledJudge*, in *SMU Law Review*, 1, 2018, 258: «*Many judges got started using Twitter for a very pragmatic reason: they have to run for election, and social media, including Twitter, is an essential campaign tool*».

31 S.L.A. Dillard - B.M. McCormack, *The Robed Tweeter. Two Judges' Views on Public Engagement*, in *Journal of Appellate Practice and Process*, 2, 2019, 197.

32 Sulla storia dei social media J. van Dijck, *The Culture of Connectivity. A Critical History of Social Media*, New York, 2013, 5 ss.; T. Tierney, *The Public Space of Social Media. Connected Cultures of the Network Society*, New York-London, 2013, 39 ss. Ovviamente, in un certo senso, tutti i "media" sono in qualche modo sempre "social": apparendo secondo alcuni tautologica la nozione di «social media», sarebbe allora più opportuno scorporare i ragionamenti intorno alla comunicazione sociale dal mezzo fisico in cui questa si manifesta (la parola, la carta stampata, internet etc.). V. in questo senso J. Hartley, *Pushing back. Social media as an evolutionary phenomenon*, in J. Burgess - A. Marwick - T. Poell (a cura di), *The SAGE Handbook of Social Media*, London, 2018, 13. Tuttavia, una simile considerazione — per certi versi "nominalistica" — nulla toglie al fatto che il senso corrente del concetto è legato a doppio con quello della connettività internet e che per questo si considerino "social media" soltanto i mezzi di comunicazioni sociale che sfruttano il *world wide web*: non è un caso, da questo punto di vista, che antesignani dei social media siano quegli stessi «bulletin board systems» da cui è derivato proprio il web. Al riguardo A. Delwiche, *Early social computing. The rise and fall of the BBS scene (1977–1995)*, in J. Burgess - A. Marwick - T. Poell (a cura di), *The SAGE Handbook of Social Media,* cit., 36. Una definizione convincente — sintetica rispetto a diversi elementi notati da altri autori — è quella di J.A. Obar - S. Wildman, *Social media definition and the governance challenge. An introduction to the special issue*, in *Telecommunications Policy*, 9, 2015, 745–747, secondo cui un social media presenta quattro caratteristiche: utilizza l'infrastruttura Web 2.0; fa dell'apporto contenutistico dell'utente la propria «linfa vitale»; è fondato sulla creazione di specifici profili che permettono di identificare un medesimo utente (non necessariamente la persona fisica che vi sta dietro) nelle sue diverse interazioni; favorisce la creazione di reti sociali degli utenti e dei gruppi. Sulle ripercussioni dell'avvento dei mezzi digitali per il generale concetto di "media", *ex plurimis* V. Zeno-Zencovich, *Il concetto di "media" nel XXI secolo*, in S. Sica - V. Zeno-Zencovich (a cura di), *Manuale di diritto dell'informazione e della comunicazione*, VI ed., Milano, 2022, 25–31, e V. Zeno-Zencovich, *Cosa intendiamo, oggi, per* media*?*, in M. Manetti - R. Borrello (a cura di), *Il diritto dell'informazione. Temi e problemi*, Modena, 2019, 11 ss.

33 «*Ce qu'un étranger comprend avec le plus de peine, aux États-Unis, c'est l'organisation judiciaire. Il n'y a pour ainsi dire pas d'événement politique dans lequel il n'entende invoquer l'autorité du juge; et il en conclut naturellement qu'aux*

centralità "politica" del potere giudiziario nella società americana, in base a cui può verosimilmente spiegarsi la circospezione degli studiosi statunitensi rispetto alle possibili "degenerazioni"[34] di quello che dovrebbe essere, tra i poteri dello Stato, «the least dangerous»[35]. Da questo punto di vista, non stupisce più di tanto, in fin dei conti, che proprio l'esperienza statunitense si mostri particolarmente solerte nell'affrontare — concettualmente, ancor prima che normativamente — le sfide e i rischi derivanti dalla diffusione dei social media.

2.2. Cenni introduttivi sulla responsabilità del giudice negli Stati Uniti

Fermo restando il rimando ai noti — benché risalenti — contributi della dottrina nazionale per un maggiore approfondimento della questione[36], pare opportuno offrire almeno un cenno introduttivo in riferimento ai sistemi di responsabilità del magistrato negli Stati Uniti. Come per tutti gli ordinamenti di *common law*, l'archetipo della responsabilità del giudice si individua nella clausola «quamdiu se bene gesserint» di cui all'*Act of Settlement* del 1701[37], che la Costituzione americana ha tradotto pressoché alla lettera stabilendo, all'art. III, sec. 1, che la carica di giudice si esercita «during good behavior». Come qualsiasi altro funzionario federale[38] — tra cui, come noto, il Presidente degli

États-Unis le juge est une des premières puissances politiques», A. de Tocqueville, *De la démocratie en Amérique*, vol. I, Paris, 1835, 164.

[34] Si pensi ad es. all'accesso dibattito scientifico intorno al problema dell'«attivismo giudiziario» (*judicial activism*), su cui v., per un'introduzione, S.A. Lindquist - F.B. Cross, *Measuring Judicial Activism*, New York, 2009, 1 ss., mentre sull'origine del concetto K.D. Kmiec, *The Origin and Current Meanings of «Judicial Activism»*, in *California Law Review*, 5, 2004, 1441 ss. In forza dell'«espansione globale del potere giudiziario», C. N. Tate - T. Vallinder (a cura di), *The Global Expansion of Judicial Power*, New York-London, 1995, è comprensibile che la categoria abbia trovato sempre più spazio anche nella letteratura italiana degli ultimi decenni: v. ad es. M. Luciani, *Funzioni e responsabilità della giurisdizione. Una vicenda italiana (e non solo)*, in *Giur. cost.*, 5, 2012, 3823; A. Baraggia, *The 'judicialization' of emergency. The case of the Eurozone Crisis*, in *Riv. dir. comp.*, 2, 2017, 87; O. Pollicino, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in *MediaLaws*, 3, 2018, 157 ss.; G. Scaccia, *Corti sovranazionali dei diritti e* judicial activism, in Id. (a cura di), *Corti dei diritti e processo politico. Convegno internazionale in memoria di Carlo Mezzanotte (Roma, 20 aprile 2017)*, Napoli, 2019, 121 ss.; A. Pin, *Rule of law, certezza del diritto e valore del precedente*, in *DPCE Online*, n. sp., 2022, 118.

[35] A. Hamilton, *The Federalist no. 78* (May 28, 1788), in A. Hamilton - J. Madison - J. Jay (a cura di), *The Federalist Papers* (1788), London, 1987, 437.

[36] S. Volterra, *L'indipendenza del giudice negli Stati degli Stati Uniti d'America,* cit., 51 ss.; J.H. Merryman, *Judicial Responsibility in the United States,* cit., 275–283; V. Vigoriti, *Le responsabilita del giudice*, cit., 91–100; V. Vigoriti, voce *Responsabilità del giudice (diritto comparato e straniero)*, in *Enc. giur.*, XXVI, Roma, 1991, 5–7; P.H. Schuck, Relazione su *Stati Uniti d'America*, in Aa.Vv., *Giurisdizione e responsabilità nei Paesi della CEE e negli Stati Uniti d'America (Roma 24-26 giugno 1987)*, Roma, 1989, 379 ss.

[37] Act of Settlement (1701) 12 & 13 Will III, c. 2. Sul ruolo della clausola per gli ordinamenti giudiziari anglo-americani, V. Varano, *Organizzazione e garanzie della giustizia civile nell'Inghilterra moderna*, Milano, 1973, 376–384; R. Rudd, *Responsibility of judges in England*, in A. Giuliani - N. Picardi (a cura di), *L'educazione giuridica*, vol. III, Perugia, 1978, 355–362; M. Cappelletti, *Giudici irresponsabili? Studio comparativo sulla responsabilità dei giudici*, Milano, 1988, 29; L. Moccia, *Il sistema di giustizia inglese. Profili storici e organizzativi*, in N. Picardi - A. Giuliani (a cura di), *L'ordinamento giudiziario*, vol. II, Rimini, 1983, 320–322.

[38] «L'*impeachment* è il mezzo col quale il poterè legislativo mantiene uno speciale controllo su tutti i

Stati Uniti — il giudice federale è dunque destituibile soltanto «on impeachment»[39]. Tuttavia, al fine di riconoscere al semplice cittadino un mezzo reattivo, estendere la cognizione al caso dell'infermità ed attuare una graduazione delle sanzioni disciplinari, il *Judicial Conduct and Disability Act* del 1980[40] ha introdotto un ulteriore regime disciplinare a livello federale, in base al quale chiunque lamenti un comportamento inappropriato o l'incapacità del giudice può oggi presentare un reclamo[41], sulla cui fondatezza si esprimerà preliminarmente il *Chief Justice* della corte di riferimento[42] e su cui poi un apposito *Special Committee* svolgerà attività di indagine[43]: competente a decidere sull'eventuale incolpazione è invece il *Judicial Council* di circuito[44], che può peraltro deferire la vicenda alla cognizione della *Judicial Conference* nazionale[45]. Rimane fermo, in ogni caso, che la destituzione del giudice federale[46] può essere disposta soltanto all'esito di procedura di *impeachment*[47], se del caso opportunamente instaurata in seguito alla trasmissione delle risultanze del procedimento disciplinare da parte della *Judicial Conference*[48].
Benché importante, la dimensione federale rappresenta comunque la punta di un iceberg la cui più vasta e interessante parte risiede al livello delle singole giurisdizioni statuali. Colpisce innanzitutto il giurista italiano che siano qui a lungo coesistiti sistemi di repressione disciplinare alternativi e concorrenti: storicamente, infatti, alla destitu-

funzionari civili dello stato: i quali sono allontanabili dall'ufficio non appena, in pratica, i due rami del Parlamento sono d'accordo circa la indegnità della persona a ricoprire il posto. Si tratta di un controllo esercitato da un organo politico e in cui la sanzione si applica in base a criteri che non sono esclusivamente giuridici», G. Bognetti, *La responsabilità per tort del funzionario e dello stato nel diritto nordamericano*, Milano, 1963, 126.

39 Che non deve considerarsi né «uno strumento di indirizzo politico» né un «procedimento giurisdizionale», quanto piuttosto un «istituto […] destinato […] al controllo dell'integrità costituzionale delle maggiori cariche pubbliche», M. Oliviero, *L'impeachment. Dalle origini inglesi all'esperienza degli Stati Uniti d'America*, Torino, 2001, 160.

40 28 U.S.C. §§ 351–364. Per un inquadramento D. Bam, *Legal process theory and judicial discipline in the United States*, in R. Devlin - S. Wildeman (a cura di), *Disciplining Judges. Contemporary Challenges and Controversies*, Cheltenham, 2021, 334 ss.

41 «Any person alleging that a judge has engaged in *conduct prejudicial to the effective and expeditious administration of the business of the courts*, or alleging that such judge is *unable to discharge all the duties of office by reason of mental or physical disability*, may file with the clerk of the court of appeals for the circuit a written complaint containing a brief statement of the facts constituting such conduct». 28 U.S.C. § 351(a) (corsivo aggiunto).

42 28 U.S.C. § 352(b). Vale la pena sottolineare, per ragionamenti che si sono svolti altrove (S.R. Vinceti, *La responsabilità disciplinare del magistrato in Irlanda. Spunti sul dibattito italiano a margine dell'istituzione del Consiglio di giustizia irlandese*, in *Diritto pubblico comparato ed europeo*, 4, 2022, 829–233) che l'eventuale "archiviazione predisciplinare" da parte del *Chief Judge* è dall'interessato impugnabile davanti al *Judicial Council* (28 U.S.C. § 352(c)).

43 28 U.S.C. § 352(a, c).

44 28 U.S.C. § 354(a, 1–2).

45 28 U.S.C. § 354(b).

46 Diverso il discorso per i «magistrate judges» e i «bankruptcy judges», per i quali, non essendo giudici costituiti ex art. III, U.S. Const., non opera la garanzia costituzionale: i secondi sono destituibili mediante decisione a maggioranza del *Judicial Council* ex 28 U.S.C. § 152(e), mentre i primi anche semplicemente a seguito di decisione della Corte del Distretto in cui esercitano la funzione ex 28 U.S.C. § 631(i).

47 28 U.S.C. § 352(a, 3(a)).

48 Cfr. 28 U.S.C. §§ 354(b), 355(b).

zione del giudice statale si poteva pervenire, tra l'altro[49], mediante «address»[50], «impeachment»[51] o «recall»[52]. Rispetto a questo coacervo di modalità, tuttavia, a partire dagli anni Sessanta del Ventesimo secolo — e precisamente nel solco dell'introduzione da parte dello Stato della California nel 1960[53] — è andato inesorabilmente affermandosi il modello delle «*permanent disciplinary commission*»[54] che, benché spesso dotate di nomi diversi, sono oggi generalmente discusse sotto la comune etichetta di «*judicial conduct commissions*»[55]. Nel tempo introdotte da tutti gli Stati americani — con emendamenti costituzionali, leggi od anche soltanto con regole di procedura delle Supreme Corti statali[56] — queste Commissioni, composte da giudici e da membri laici, sono oggi il "cuore" della giustizia disciplinare, con la pressoché totale desuetudine degli altri metodi. Benché i regimi giuridici delle *judicial conduct commission* varino nei diversi Stati, ciò che le differenzia dai *judicial council* federali è la capacità di irrogare qualsiasi provvedimento disciplinare, compresa la destituzione: in alcune giurisdizioni il provvedimento

[49] Sono anche annoverati come metodi di repressione disciplinare — benché più problematicamente — la destituzione per iniziativa del governatore dello Stato, E.J. Schoenbaum, *A Historical Look at Judicial Discipine*, in *Chicago-Kent Law Review*, 1, 1977, 3–4), la rimozione derivante dalla mancata conferma del giudice nella carica (cfr. Note *Remedies for Judicial Misconduct and Disability. Removal and Discipline of Judges*, in *New York University Law Review*, 1, 1966, 171; R.R. Wheeler - A.L. Levin, *Judicial Discipline and Removal in the United States*, Washington, 1979, 8; E.J. Schoenbaum, *A Historical Look at Judicial Discipine,* cit., 9–10), l'assegnazione del giudice ad una sede indesiderata (R.R. Wheeler - A.L. Levin, *Judicial Discipline and Removal in the United States,* cit., 13–14; *Remedies for Judicial Misconduct*, cit., 173–174). In riferimento alla dimensione federale C.G. Geyh, *Informal Methods of Judicial Discipline*, in *University of Pennsylvania Law Review*, 1, 1993, 243 ss. Richiamando più largamente «impeachment», «address» e «recall» come «metodi tradizionali» si segue l'impostazione di S. Volterra, *L'indipendenza del giudice negli Stati degli Stati Uniti d'America,* cit., 51 ss., part. 58, 151.

[50] Entrambe le camere dell'organo legislativo approvano una risoluzione che richiede formalmente al potere esecutivo — dunque, il governatore — di rimuovere un particolare giudice, senza peraltro la necessaria indicazione dei fatti di rilevanza disciplinare. E.J. Schoenbaum, *A Historical Look at Judicial Discipine,* cit., 4–5; *Remedies for Judicial Misconduct,* cit., 164; R.R. Wheeler - A.L. Levin, *Judicial Discipline and Removal in the United States,* cit., 7; nella letteratura italiana cfr. S. Volterra, *L'indipendenza del giudice negli Stati degli Stati Uniti d'America,* cit., 66–73.

[51] Diversamente dall'*address*, nell'*impeachment* una delle due camere parlamentari delibera le specifiche accuse disciplinari rivolte al giudice, sulla cui effettività sarà chiamata a pronunciarsi l'altra camera. Cfr. *Remedies for Judicial Misconduct*, cit., 163; R.R. Wheeler - A.L. Levin, *Judicial Discipline and Removal in the United States,* cit., 7; E.J. Schoenbaum, *A Historical Look at Judicial Discipine,* cit., 5–8, nonché S. Volterra, *L'indipendenza del giudice negli Stati degli Stati Uniti d'America,* cit., 59–66.

[52] In questo caso, al raggiungimento di un determinato quorum una petizione popolare è sottoposta all'elettorato al fine di decidere l'eventuale rimozione del giudice. E.J. Schoenbaum, *A Historical Look at Judicial Discipine,* cit., 8–9; R.R. Wheeler - A.L. Levin, *Judicial Discipline and Removal in the United States,* cit., 8; *Remedies for Judicial Misconduct*, cit., 164–165, e sempre S. Volterra, *L'indipendenza del giudice negli Stati degli Stati Uniti d'America,* cit., 73 ss.

[53] R.R. Wheeler - A.L. Levin, *Judicial Discipline and Removal in the United States*, cit., 22–24; E.J. Schoenbaum, *A Historical Look at Judicial Discipine,* cit., 19–22; J.H. Merryman, *Judicial Responsibility in the United States,* cit., 278–280. L'introduzione, beninteso, ha rappresentato l'esito di una lunga fase di gestazione che ha visto dapprima il coinvolgimento delle associazioni professionali, E.J. Schoenbaum, *A Historical Look at Judicial Discipine,* cit., 10–13 e poi la sperimentazione di procedimenti a cognizione esclusivamente giudiziale (ivi, 13–19) che suscitarono, tuttavia, «[*f]ears* […] *that judges would have a tendency to whitewash misconduct by their colleagues if the responsibility of discipline were left to them alone*» (ivi, 19).

[54] S. Volterra, *L'indipendenza del giudice negli Stati degli Stati Uniti d'America,* cit., 141 ss.

[55] C. Gray, *How Judicial Conduct Commissions Work*, in *The Justice System Journal*, 3, 2007, 405.

[56] Ivi, 407.

disciplinare diventa efficace soltanto nel momento in cui sia fatto proprio dalla corte suprema statale, in altre è definitivo benché soggetto ad appello davanti alla stessa corte suprema e in altre ancora il regime varia a seconda che si tratti di un rimprovero o di una censura, ovvero consista in una sospensione o della rimozione[57].

Detto dell'*auctoritas*, occorre fare poi brevemente accennare al *quid* della responsabilità disciplinare: gli standard di comportamento che devono essere rispettati dai giudici nei diversi Stati[58]. Benché in ragione del pieno federalismo in materia di organizzazione della giustizia ogni Stato sarebbe astrattamente legittimato a stabilire autonome fattispecie disciplinari, si osserva una sostanziale convergenza tra gli standard previsti nelle diverse realtà. L'uniformità non è un caso, ma deriva dalla redazione dei «Canons of Judicial Ethics» da parte dell'American Bar Association (ABA) nel 1924, cui hanno fatto seguito svariate versioni — nel 1972, nel 1990, nel 2007 — fino ad arrivare all'*ABA Model Code of Judicial Conduct* (*Model Code*) odierno, rivisto nel 2010: pur trattandosi di un modello di normazione redatto da un'associazione privata e dunque privo di immediato valore giuridico[59], il *Model Code* è stato preso a riferimento nell'adozione dei codici disciplinari di tutti gli Stati, al punto che le divergenze sono più spesso spiegabili in forza dell'aggiornamento o meno del codice statale all'ultima edizione del modello, piuttosto che in funzione di vere e proprie scelte ordinamentali differenti, comunque esistenti[60]. Potendo dunque considerare il modello ABA rappresentativo dei codici statali, ciò che emerge *ictu oculi* è la spiccata indeterminatezza degli standard, articolati in quattro canoni generali[61], entro cui sono poi previste sottoregole in alcuni casi più specifiche[62]: laddove l'ordinamento italiano ha optato, non senza incoerenze,

---

[57] Ivi, 416–417.

[58] S. Volterra, *L'indipendenza del giudice negli Stati degli Stati Uniti d'America,* cit., 92–97.

[59] «*The 1972, 1990, and 2007 Codes, like the 1924 Canons of Judicial Ethics, are models only; they have no legal effect unless enacted as a statute or court rule by the various jurisdictions throughout the nation*», C.G. Geyh - J.J. Alfini - J. Sample, *Judicial Conduct and Ethics*, New York, 2020, § 1.03.

[60] «*Every state and the District of Columbia now has a code based on one of the three ABA models. The widespread adoption of state codes based on one of the three ABA Codes provides a degree of uniformity from jurisdiction to jurisdiction and forms the foundation for a national body of law concerning judicial conduct. The vast majority of judges, both state and federal, are subject to a code of conduct with uniform general principles and relatively specific rules, some of which are uniform and others of which vary from jurisdiction to jurisdiction*» (*ibidem*).

[61] I quattro canoni rispettivamente sanciscono che «*[a] judge shall uphold and promote the independence, integrity, and impartiality of the judiciary, and shall avoid impropriety and the appearance of impropriety*», che «*[a] judge shall perform the duties of judicial office impartially, competently, and diligently*», che «*[a] judge shall conduct the judge's personal and extrajudicial activities to minimize the risk of conflict with the obligations of judicial office*», e che «*[a] judge or candidate for judicial office shall not engage in political or campaign activity that is inconsistent with the independence, integrity, or impartiality of the judiciary*» (cfr. Model Code, Canons 1–4).

[62] Mentre le sottoregole dei primi due canoni non sembrano in grado di mutare il giudizio di astrattezza dei valori ivi menzionati, forse perché riferibili a materie precise — le attività extragiudiziali e l'attività politica — il terzo e quatto canone contengono indicazioni in qualche modo specifiche. Così, ad es., in riferimento alle attività extragiudiziali incompatibili con la carica si prevedono divieti disciplinari specifici, avvicinabili per certi versi alla tipizzazione disciplinare italiana: dal divieto di apparire come esperto davanti ad organi governativi, salvo che per questioni come l'amministrazione della giustizia, il sistema giuridico, ovvero qualora il giudice abbia una specifica competenza in materia (Rule 3.2), al divieto di affiliazione ad organizzazioni discriminatorie (Rule 3.6) o alla regolamentazione dell'accettazione di ragionevoli liberalità (Rule 3.13).

per un tentativo di tipizzazione dell'illecito disciplinare[63], gli ordinamenti statunitensi — come tutti i sistemi di *common law* — si possono così considerare una mezza via rispetto alle laconiche formule vigenti in altri ordinamenti di *civil law*[64].

In ultimo, per il particolare ruolo che tale fonte del diritto dispiega nella regolamentazione dei social media, è opportuno un cenno al ruolo delle *advisory opinion*. Adottate da organismi costituiti con diverse denominazioni presso le commissioni disciplinari ovvero presso le corrispondenti Corti supreme[65], le *advisory opinion* sono la risposta ad un dubbio di un giudice riguardo all'applicazione degli standard di condotta giudiziaria ad un particolare frangente o ad una situazione ipotetica, di portata più o meno generale[66]. Proprio per la natura anticipatoria e consultiva rispetto all'illecito disciplinare, le *advisory opinion* hanno rappresentato il primo e più importante formante con cui si è trattata la questione dell'uso dei social media da parte dei giudici[67]. Tuttavia, come si è ricordato proprio nel contesto della discussione di uno specifico social media, benché

[63] Di «tipizzazione» dell'illecito disciplinare parla generalmente la dottrina — per certi versi "inevitabilmente", ché quello era l'espresso intento del legislatore delegante *ex* art. 2, c. 6, lett a), della l. 25 luglio 2005, n. 150 — in riferimento al d.lgs. 23 febbraio 2005, n. 109: v. *ex plurimis* G. Ferri, *La magistratura in Italia*, Torino, 2018, 173. Tuttavia, come rilevano altri autori, la presenza di «norme "di chiusura"» e «disposizioni […] "a fattispecie aperta"» renderebbe forse preferibile parlare di «predeterminazione» disciplinare, più che di «vera e propria tipizzazione degli illeciti» (F. Biondi, *La responsabilità disciplinare. Problemi vecchi e nuovi*, in F. Grandi (a cura di), *Il Consiglio superiore della Magistratura: snodi problematici e prospettive di riforma. Atti del Seminario annuale dell'Associazione Gruppo di Pisa, 23 ottobre 2020, online*, Napoli, 2021, 44). V. altresì sul tema F. Dal Canto, *Lezioni di ordinamento giudiziario*, II ed., Torino, 2020, 281, che parla di «una tipizzazione "tendenzialmente rigida"», nonché, specie in riferimento alla clausola di «scarsa rilevanza del fatto», A. Caputo, *La tipizzazione dell'illecito disciplinare del magistrato ordinario*, in G. Campanelli (a cura di), *Indipendenza, imparzialità e responsabilità dei giudici speciali*, cit., 183 ss., spec. 206–211. In generale, sul bilancio della tipizzazione della responsabilità disciplinare, D. Cavallini, *Gli illeciti disciplinari dei magistrati ordinari prima e dopo la riforma del 2006*, Padova, 2011, 29 ss.; Id., *La responsabilità disciplinare dei magistrati*, in G. Di Federico (a cura di), *Ordinamento giudiziario. Uffici giudiziari, CSM e governo della magistratura*, Bologna, 2019, 371 ss.

[64] Per citare due esempi, in Francia l'art. 43 dell' Ordonnance n° 58–1270 du 22 décembre 1958 dispone che «[t]out manquement par un magistrat aux devoirs de son état, à l'honneur, à la délicatesse ou à la dignité, constitue une faute disciplinaire», mentre in Germania, oltre agli obblighi cui soggiace in quanto *Beamte*, il giudice federale «hat sich innerhalb und außerhalb seines Amtes, auch bei politischer Betätigung, so zu verhalten, daß das Vertrauen in seine Unabhängigkeit nicht gefährdet wird» ex art. 39, Deutsches Richtergesetz (19 April 1972). Sulla responsabilità del giudice in Francia cfr. F. Terré, *La responsabilité des juges en droit français*, in A. Giuliani - N. Picardi (a cura di), *L'educazione giuridica*, vol. III, Perugia, 1978, 460, V. Vigoriti, *La responsabilità del giudice. Orientamenti e prospettive nell'esperienza italiana e comparata*, in *Quad. cost.*, 1, 1983, 61–62, e soprattutto A. De Vita, *A mali estremi prudenti rimedi. La responsabilità del giudice nel diritto francese tra l'eredità del passato e le soluzioni del regime odierno*, in *Quadrimestre*, 3, 1985, 427–434, che parla di «termini pericolosamente generici» della formula, capace di esporre il giudice agli «arbitri dell'azione disciplinare ai condizionamenti dei preconcetti e dei conformismi dominanti nelle più svariate sfere della vita sociale» (ivi, 432, 434); sulla Germania cfr. W. Grunsky, *La responsabilità del giudice nel diritto tedesco*, in A. Giuliani - N. Picardi (a cura di), *L'educazione giuridica*, vol. III, Perugia, 1978, 235–237.

[65] V. ad es. il caso dell'Arkansas in cui la *Judicial Ethics Advisory Committee* è parte della *Judicial Discipline and Disability Commission*, che ne nomina i membri. Al contrario, cfr. ad. es. il caso della *Committee on Judicial Ethics Opinions* costituita presso la *California Supreme Court*, che ne elegge i componenti.

[66] Cynthia Grey ricorda, ad es., il caso di un giudice di New York che chiese alla *Advisory Committee on Judicial Ethics* se fosse lecito accettare un lascito testamentario di mille dollari per svolgere un evento sociale presso il tribunale, invitandovi gli avvocati del foro (C. Gray, *Helping Judges Look before They Leap. Judicial Ethics Advisory Committees*, in *Court Review*, 4, 2018, 152).

[67] Cfr. ivi, 153–154.

le *advisory opinion* abbiano valore orientativo capace di creare affidamento sull'agire futuro degli organi disciplinari[68] e in questo senso acquisiscano un "valore precedenziale", rimangono prive di applicabilità diretta in giudizio[69]. Peraltro, proprio per il fatto che l'*advisory opinion* sia richiesta spontaneamente dal giudice e che la *voluntary disclosure* di un fatto di potenziale rilevanza disciplinare sia generalmente foriera di un trattamento più favorevole da parte delle commissioni disciplinari, il rischio è che le *advisory opinion* finiscano per ingenerare un'impressione di falsa permissività[70]. Ciononostante, il costante richiamo nell'embrionale giurisprudenza disciplinare conferma l'importanza delle *advisory opinion* nelle diverse giurisdizioni[71], spiegando la concentrazione della dottrina statunitense sull'analisi del formante in questione.

2.3. Categorizzazione degli approcci normativi

2.3.1. Approcci restrittivi

Un modo efficace per sistematizzare le diverse regolamentazioni della materia consiste nel giustapporre gli approcci "restrittivi" all'utilizzo dei social media da parte dei magistrati a quelli più "aperturisti"[72]. Archetipo del primo tipo deve senz'altro considerarsi la regolamentazione dello Stato della Florida[73], che con una *Opinion* del 2009[74] pur risolvendo favorevolmente altri quesiti[75] ha sancito il divieto per qualsiasi giudi-

[68] «*These opinions provide probative value in predicting the way courts will handle Facebook in disciplinary actions and cases, but it is still important to keep in mind their purely advisory nature*» (D. Smith, *When Everyone is the Judge's Pal. Facebook Friendship and the Appearance of Impropriety Standard*, in *Case Western Reserve Journal of Law, Technology & the Internet*, 1, 2012, 24).

[69] «[*W*]*hile advisory opinions have some precedential value, they are generally not binding in court*» (*ibidem*).

[70] «*It is perfectly conceivable that even a jurisdiction with a relatively lenient advisory opinion concerning Facebook friendships could come down hard on a judge if an ethical case arose and there was no disclosure*» (*ibidem*).

[71] V. ad es. *Youkers v. State*, 400 S.W.3d 200, 205 (Tex. App. 2013); *In re Slaughter*, 480 S.W.3d 842, 848 (Tex. Spec. Ct. Rev. 2015); *In re Whitmarsh*, 10 (N.Y. Comm. Jud. Conduct, December 28, 2016); *Urie*, *Order* (Arizona Comm. Jud. Conduct, June 12, 2018).

[72] A. O'Brien, *Are Attorneys and Judges One Tweet, Blog or Friend Request Away from Facing a Disciplinary Committee?*, in *Loyola Journal of Public Interest Law*, 2, 2010, 525 ss.; S.V. Jones, *Judges, Friends, and Facebook. The Ethics of Prohibition*, in *Georgetown Journal of Legal Ethics*, 2, 2011, 286 ss.; N.J. Mitchell, *Judge 2.0. A New Approach to Judicial Ethics in the Age of Social Media*, in *Utah Law Review*, 4, 2012, 2133 ss.; C. Estlinbaum, *Social Networking and Judicial Ethics*, in *St. Mary's Journal on Legal Malpractice and Ethics*, 1, 2012, 15 ss.; J.G. Browning, *Why Can't We Be Friends? Judges' Use of Social Media*, in *University of Miami Law Review*, 2, 2014, 510 ss.; M.S. Kurita, *Electronic Social Media. Friend or Foe for Judges,* cit., 200 ss.

[73] «Florida has arguably been the most vocal about ethical problems created by judicial Facebook friendships, and has certainly taken the strongest stance» (D. Smith, *When Everyone is the Judge's Pal. Facebook Friendship and the Appearance of Impropriety Standard,* cit., 24–25).

[74] Fla. Sup. Ct., Ethics Advisory Comm., Opinion 2009–20 (November 17, 2009).

[75] La Commissione ha infatti affermato tanto il diritto del magistrato a postare propri contenuti sui social media — nei limiti in cui questi non siano altrimenti in contrasto con il codice disciplinare — quanto la libertà dei team che coordinano le campagne elettorali dei giudici di postare materiale nel sito dedicato all'elezione del giudice, nonché di permettere ad altre persone — tra cui anche gli avvocati che potrebbero in futuro apparire davanti al giudice (!) — di dichiararsi fan o sostenitori del candidato sul sito, ma solo fintantotchè l'aspirante giudice o il suo team non possano controllare chi decide di iscriversi (*idest*, l'*endorsement* non è rigettabile dal ricevente). Cfr. *ibidem*.

ce di intrattenere un "amicizia" su Facebook con avvocati che potrebbero trovarsi a patrocinare davanti al magistrato, in quanto ciò ingenera «the impression that these lawyer "friends" are in a special position to influence the judge»[76]. Ad essere stigmatizzata non è stata dunque l'effettività dell'influenza indebita mediante il social media — è del resto esperienza comune, che non sfuggiva al *Committee*, che le "amicizie" su Facebook possano essere assolutamente formali, generiche, del tutto irriducibili ad una vera e propria amicizia — quanto la lesione "sempre e comunque" dell'*apparenza* di imparzialità[77]. Benché in tempi più recenti non siano mancate indicazioni di uno stemperamento dell'approccio[78], il divieto rimane vigente e continua ad assegnare alla Florida "la palma" di «most draconian of jurisdictions when it comes to judges and social media»[79].

Questo netto giudizio sull'esperienza della Florida ha senso, tuttavia, soltanto in una prospettiva diacronica, giacché anche altri Stati hanno in seguito adottato approcci similmente "prudenziali", giungendo addirittura ad estendere il divieto di amicizia a tutte le persone «who regularly appear before the judge in an adversarial role»[80]. Questo è il caso dello Stato dell'Oklahoma che, rovesciando "polemicamente" il ragionamento del più aperturista Stato del Kentucky ha innanzitutto ricordato nella sua *Opinion* che in ragione della cruciale importanza della fiducia collettiva nell'imparzialità e correttezza della magistratura «*is imperative to err on the side of caution where the situation is "fraught with peril"*»[81]; a quanti potrebbero contestare l'eccessiva compressione dei diritti del giudice, l'*Opinion* risponde che la speciale natura della funzione esercitata rende necessaria l'imposizione di restrizioni e cautele aliene alla generalità dei cittadini[82]. Per conseguenza, il giudice dell'Oklahoma può stringere amicizia su Facebook con qualsiasi soggetto di norma estraneo ai suoi processi — sempreché, s'intende, l'utilizzo del social media non sia in altro modo lesivo del Codice di condotta[83].

Pur fissando lo stesso tipo di divieto, lo Stato del Connecticut ha impostato la questione in riferimento alla globalità dei "social media", cercando di stabilire indicazioni utili

---

[76] *Ibidem*.

[77] L'introduzione dello standard dell'«*appearance of impropriety*» nel *Model Code* del 2007 è stata ragione di divisione tra i commentatori, nonché all'interno della stessa ABA: N.J. Moore, *Is the Appearance of Impropriety an Appropriate Standard for Disciplining Judges in the Twenty-First Century?*, in *Loyola University Chicago Law Journal*, 2, 2009, 285–286.

[78] Cfr. *Law Offices of Herssein and Herssein v. United Services Automobile Association*, 271 So. 3d 889 (Fla. Nov. 15, 2018). *Contra* v. *Domville v. State,* 103 So. 3d 184, 186 (Fla. Dist. Ct. App. 2012). Nota il contrasto tra la *advisory opinion* del 2009 e la decisione del 2018 C. Gray, *Social Media and Judicial Ethics Up-date*, gennaio 2023, 25.

[79] J.G. Browning, *Why Can't We Be Friends?*, cit., 491. Nello stesso senso A. O'Brien, *The Judicial Process. Law, Courts, and Judicial Politics,* cit., 527; C. Estlinbaum, *Social Networking and Judicial Ethics*, in *St. Mary's Journal on Legal Malpractice and Ethics,* cit., 17; D. Smith, *When Everyone is the Judge's Pal. Facebook Friendship and the Appearance of Impropriety Standard,* cit., 24–45; M.S. Kurita, *Electronic Social Media. Friend or Foe for Judges* cit., 228, che parla della Florida come del «leader of the restrictive opinions».

[80] C. Gray, *Social media and judicial ethics. Part I*, Spring 2017, 17.

[81] Okla. Jud. Ethics Advisory Panel, Opinion 2011–3 (July 6, 2011), § 9

[82] «*A Judge must accept restrictions on the Judge's conduct that might be viewed as burdensome by the ordinary citizen and should do so freely and willingly*» (ivi, § 10).

[83] Ivi, § 7.

al di là dell'esperienza di Facebook. Ricordando che la partecipazione ai social media da parte del giudice è «fraught with peril»[84] il Connecticut ha esplicitato una serie di ulteriori divieti, tra cui si possono ricordare: l'obbligo di mantenere la dignità della professione in ogni interazione sul social media; il divieto di esternazioni atte ad erodere la fiducia sull'imparzialità e indipendenza del giudizio[85]; il divieto di diffusione di materiale che potrebbe sembrare finalizzato ad avanzare interessi propri del giudice o di altri soggetti specifici[86]; il divieto di associazioni formali con persone o organizzazioni che, in qualsiasi modo, possano poi apparire in posizione di "speciale influenza" sul giudice[87]; il divieto di commenti su questioni pendenti davanti al magistrato, nonché di ricerche indipendenti sulle parti o sui testimoni; il divieto di prendere parte a qualsiasi tipo di attività politica [88], tra cui a titolo esemplificativo sono annoverate l'espressione di sostegno od opposizione ad un soggetto candidato ad una qualsiasi carica pubblica, l'apprezzamento per specifici partiti politici, ovvero l'adozione di commenti o osservazioni su specifiche riforme legislative o comunque temi politicamente sensibili[89].
A testimonianza, peraltro, dell'insufficienza epistemica di una possibile distinzione tra Stati "conservatori" e Stati "progressisti" in riferimento al problema *de quo*, altro caso interessante è l'approccio restrittivo adottato dallo Stato del Massachusetts, ove sono attualmente vigenti tre diverse regolamentazioni per Facebook, Twitter e Linkedin[90]. Benché infatti il *Committee on Judicial Ethics* del Massachusetts abbia stemperato il proprio approccio — affievolendo l'obbligo di monitoraggio da parte del giudice sulle opinioni espresse dalle proprie conoscenze online che possano astrattamente infirmare l'apparenza di «integrity or impartiality of the judiciary» e abrogando la raccomandazione all'occultamento della propria identità di giudice sulla piattaforma — è stato invece confermato il divieto di amicizia con avvocati che possano apparire davanti al giudice. Ciò che risulta particolarmente interessante, tuttavia, è proprio l'attenzione alle specificità degli altri social media. Sebbene infatti anche in riferimento a Linkedin si sia affermato l'obbligo del giudice di rifiutare richieste di connessione con avvocati che verosimilmente potrebbero patrocinare davanti a lui in giudizio, la conclusione è stata raggiunta prendendo in considerazione la natura "professionale" di Linkedin — non semplicemente traslando le considerazioni sviluppate in riferimento al più informale Facebook[91]. Questa sensibilità tecnologica dell'autorità normativa emerge con ancora

[84] Conn. Comm Jud. Ethics, Opinion 2013–6 («*Extrajudicial Activities; Electronic Social Media; Facebook*») (March 22, 2013).

[85] *Ibidem.*

[86] *Ibidem.*

[87] *Ibidem.*

[88] *Ibidem.*

[89] *Ibidem.*

[90] Prima della revisione degli standard disciplinari operata dalla Corte Suprema del Massachusetts nel 2011, era stata adottata una *Opinion* concernente Facebook, da ritenersi oggi non più applicabile, che richiamando l'impostazione della Florida giungeva alle stesse conclusioni sull'utilizzabilità della piattaforma e sul divieto di amicizia dei giudici con «attorneys who may appear before them». Cfr. Mass. Comm. Jud. Ethics, Opinion 2011–6 («*Facebook: Using Social Networking Website*») (December 28, 2011).

[91] Mass. Comm. Jud. Ethics, Opinion 2016–08 (September 6, 2016) («*Linked In: Using Social Networking Site*»)

maggiore evidenza davanti alla regolamentazione di Twitter, rispetto a cui, pur senza pretese di esaustività, è stata adottata una lista di specifiche modalità di interazione permesse e vietate, che ribadiscono la generale prudenza adottata dalla Commissione[92].

2.3.2. Approcci aperturisti

Al contrario, le *ethics opinion* di altri Stati si segnalano per un approccio più aperturista verso l'utilizzo dei social media da parte dei magistrati. Per il richiamato ruolo di paradigma normativo, può avere un senso far partire la discussione dall'approccio dell'ABA, che pure ha preso posizione solo successivamente all'adozione delle regolamentazioni di alcuni Stati. Benché consapevole dei rischi per l'indipendenza, l'imparzialità e la fiducia del pubblico nella magistratura, l'*Opinion* ABA del 2013 esordisce innanzitutto con una nota positiva, riconoscendo che i social media possano risultare un utile strumento per evitare che i giudici siano percepiti come «isolated or out of touch»[93]. In particolare sono due gli aspetti su cui l'*Opinion* prende una posizione specifica: da una parte, l'ABA esclude che la semplice amicizia sul social media tra il giudice e l'avvocato che possa patrocinare avanti al giudice sia elemento di per sé solo sufficiente a far dubitare dell'imparzialità del magistrato, dal momento che la «[s]*imple designation as an ESM connection does not, in and of itself, indicate the degree or intensity of a judge's relationship with a person*». Dall'altra parte, l'ABA riconosce l'utilizzabilità dei social media nelle campagne elettorali dei giudici a condizione che i siti non siano amministrati direttamente dal giudice o dal candidato[94], al tempo stesso proibendo ai giudici di esprimersi — in positivo o in negativo — su qualsiasi altro candidato a qualsiasi carica pubblica[95].
Tra gli Stati che hanno adottato un approccio aperturista — innanzitutto riconoscendo la liceità dell'amicizia sui social media tra giudice e avvocato — possono annoverarsi Kentucky[96], Maryland[97], New Mexico[98], New York[99], South Carolina[100], Ohio[101] e Utah[102].

---

92 Cfr. Mass. Comm. Jud. Ethics, Opinion 2016–09 (November 22, 2016) («*Twitter: Using Social Networking Site*»).

93 ABA, Formal Opinion 462 (February 21, 2013) («*Judge's Use of Electronic Social Networking Media*»).

94 Ivi, 4.

95 *Ibidem*.

96 Ky. Jud. Ethics. Comm., Opinion 2010–119 (January 20, 2010) («*Judges' Membership on Internet-Based Social Networking Sites*»).

97 Md. Jud. Ethics Comm., Formal Opinion 2012–07 (June 12, 2012) («*Judge Must Consider Limitations on Use of Social Networking Sites*»).

98 N.M. Advisory Comm. C. Jud. Conduct, Opinion (February 15, 2016) («*Advisory Opinion Concerning Social Media*»).

99 N.Y. St. Advisory Comm. Jud. Ethics, Opinion 08–176 (January 29, 2009).

100 S.C. Advisory Comm. Standards Jud. Conduct, Opinion 17–2009 (October, 2009) («*Propriety of a magistrate judge being a member of a social networking site such as Facebook*»).

101 Sup. Ct. Ohio Bd. of Comm'rs Grievances and Discipline, Opinion 2010–7 (December 3, 2010).

102 Utah Ethics Advisory Comm., Opinion 12–01 (August 31, 2012) («*Judges and Social Media*»).

Tra questi, la «most liberal stance»[103] può attribuirsi alla South Carolina[104], che nell'affermare la possibile amicizia su Facebook tra magistrato e agente di polizia ha esplicitamente incoraggiato l'uso dei social media da parte dei giudici onde evitare che questi rimangano «*isolated from the community in which the judge lives*»: da questo punto di vista, afferma l'*Opinion* del South Carolina, la partecipazione ai social media dovrebbe rendere il magistrato più simpatetico e intellegibile agli occhi della comunità in cui esercita la sua giurisdizione[105]. Di recente, poi, il medesimo *Advisory Committee* ha dichiarato la piena utilizzabilità dei social media nel contesto delle campagne elettorali[106].

Diacronicamente, tuttavia, l'esperienza di riferimento è quella della *New York State Commission on Judicial Ethics*, cui si deve peraltro la prima regolamentazione *tout court* dell'utilizzo dei social media da parte dei magistrati[107]. Riconoscendo le diverse ragioni per cui il giudice potrebbe nutrire il legittimo desiderio di prendere parte ad un social media[108], nel 2008 la Commissione affermò che non v'era niente di «inherently inappropriate» nella partecipazione attiva di un giudice ad un social media, almeno fintantoché i magistrati avessero adottato il giusto livello di «*prudence, discretion and decorum*»[109]. La sensibilità per il tema è dimostrata dal numero di volte in cui la Commissione è poi tornata sull'argomento: nel 2013, recuperando una precedente distinzione tra diverse tipologie di relazione — «*acquaintance*», «*close social relationship*», «*close personal relationship*»[110] — ha affermato che in sé e per sì il fatto di essere «"Facebook friend"» è insufficiente a giustificare la ricusazione[111]; nel 2014 ha invece vietato l'*hosting* della pagina ufficiale di un Tribunale su Facebook temendo l'associabilità delle pubblicità (gestite dal social media) e l'istituzione giudiziaria[112]; nel 2020 ha scoraggiato i giudici *lato sensu* "onorari" — praticanti l'attività forense — dal pubblicizzare le proprie decisioni sui social media[113]; nel 2021 ha vietato la partecipazione ufficiale del giudice ad attività di raccolta fondi

---

[103] Così D. Smith, *When Everyone is the Judge's Pal. Facebook Friendship and the Appearance of Impropriety Standard,* cit., 27.

[104] Cfr. A. O'Brien, *The Judicial Process. Law, Courts, and Judicial Politics,* cit., 252–526; S.V. Jones, *Judges, Friends, and Facebook. The Ethics of Prohibition*, in *Georgetown Journal of Legal Ethics,* cit., 288; S. Singh, *Friend Request Denied. Judicial Ethics and Social Media*, in *Case Western Reserve Journal of Law, Technology and the Internet*, 1, 2016, 169.

[105] «Allowing a Magistrate to be a member of a social networking site allows the community to see how the judge communicates and gives the community a better understanding of the judge» (S.C. Advisory Comm. Standards Jud. Conduct, Opinion 17–2009, cit.).

[106] S.C. Advisory Comm. Standards Jud. Conduct, Opinion 4–2022 (March 11, 2022).

[107] C. Estlinbaum, *Social Networking and Judicial Ethics*, in *St. Mary's Journal on Legal Malpractice and Ethics,* cit., 15.

[108] «*There are multiple reasons why a judge might wish to be a part of a social network: reconnecting with law school, college, or even high school classmates; increased interaction with distant family members; staying in touch with former colleagues; or even monitoring the usage of that same social network by minor children in the judge's immediate family*» (N.Y. St. Advisory Comm. Jud. Ethics, Opinion 08–176).

[109] *Ibidem*.

[110] N.Y. St. Advisory Comm. Jud. Ethics, Opinion 11–125 (October 27, 2011).

[111] N.Y. St. Advisory Comm. Jud. Ethics, Opinion 13–39 (May 28, 2013) (corsivo aggiunto sostituisce grassetto in originale).

[112] N.Y. St. Advisory Comm. Jud. Ethics, Opinion 14–05 (March 13, 2014).

[113] N.Y. St. Advisory Comm. Jud. Ethics, Opinion 20–58 (April 30, 2020).

attraverso i social media, anche se organizzate da associazioni senza scopo di lucro[114].
Infine, merita di essere segnalata l'esperienza della California. Si tratta di una vicenda significativa perché qui, a causa della soltanto recente costituzione dell'organo di *advisory* disciplinare[115] il tema è stato trattato in prima battuta dall'associazione professionale dei magistrati con un pronunciamento privo di rilevanza giuridica esterna[116]. Con la discussa[117] *Opinion* 66 del 2010[118] il *Judicial Ethics Committee* della *California Judges Association* ha infatti stabilito che i giudici potevano stabilire "un'amicizia" sui social media con avvocati che avrebbero potuto patrocinare davanti a loro solo a condizione che l'avvocato venisse «unfriend[ed]» in caso di effettiva pendenza di una lite davanti al magistrato[119] e che non risultasse comunque pregiudicata l'apparenza di imparzialità e inappropriatezza all'esito di un'analisi "contestuale" fondata su specifici indici: la natura del social media, il numero di "amicizie" del giudice, la "politica" adottata dal giudice nell'ammettere nuovi amici e la frequenza con cui l'avvocato potrebbe patrocinare davanti al magistrato in questione[120]. In tempi più recenti, insieme ad un ulteriore intervento della *California Judges Association*[121] il neocostituito *Committee on Judicial Ethics Opinions* (CJEO) della *California Supreme Court* ha preso posizione sul tema: dapprima il CJEO ha perimetrato i profili di responsabilità del giudice d'appello per commenti inappropriati esternati sui social media dai membri del proprio staff[122]; ancor più interessante, tuttavia, è l'*Opinion* del 2021 in cui, pur affermando la liceità delle osservazioni sulla disciplina vigente o sulle proposte di riforma, l'organo di *advisory* disciplinare ha rimarcato la necessità di evitare valutazioni che potrebbero essere comunque percepite come un «prohibited political commentary»[123] idoneo a mettere in dubbio l'imparzialità del magistrato[124].

---

114 N.Y. St. Advisory Comm. Jud. Ethics, Opinion 21–31 (March 11, 2021).

115 Anche se spesso costituto presso di essa, l'ente di *advisory* disciplinare non coincide con la Commissione disciplinare, per la cui introduzione, come richiamato *supra* § 2.2, la California è stata invece esperienza apripista.

116 «*The opinions of the California Judges Association, while useful to the state's judiciary, are educational rather than binding*» (N.J. Mitchell, *Judge 2.0. A New Approach to Judicial Ethics in the Age of Social Media,* cit., 2133, nota 38). Per certi versi si tratta di un vincolo assimilabile a quello della responsabilità deontologica dei magistrati iscritti all'ANM.

117 Cfr. B. Hull, *Why Can't We Be «Friends»? A Call for a Less Stringent Policy for Judges Using Online Social Networking*, in *Hastings Law Journal*, 2, 2012, 617 ss.

118 Cal. Judges Ass'n Jud. Ethics Comm., Opinion 66 (November 23, 2010).

119 Ivi, 3.

120 Ivi, 8.

121 In cui è stata affermata l'utilizzabilità di social media finalizzati a «crowdsourced reviews» — l'esempio erano Yelp e Tripadvisor — ovvero che permettessero di apporre «like» ad altre pagine (cfr. Cal. Judges Ass'n Jud. Ethics Comm., Opinion 78 (January 2020)).

122 Cal. Sup. Ct. Comm. Jud. Ethics, Oral Advice Summary 2020–037 (October 23, 2020) («*Judicial Obligations Relating to Social Media Comments by Appellate Court Staff*»).

123 Cal. Sup. Ct. Comm. Jud. Ethics, Expedited Opinion 2021–042 (April 28, 2021) («*Social Media Posts About the Law, the Legal System, or the Administration of Justice*»), 9.

124 Ivi, 4.

2.4. I nodi fondamentali del problema

Un dato che sembra caratterizzare la letteratura statunitense sul tema che ci impegna è il definitivo consenso, oggi[125], sull'irriducibilità del fenomeno "social media" alle tradizionali forme dell'illecito disciplinare. Si è innanzitutto constatato come, da un punto di vista quantitativo, la socialità online funga da «moltiplicatore» di comportamenti reprensibili, verosimilmente a causa di quel un più generale «online disinhibition effect» che accompagna i social media[126]. Né pare possibile giustificare questa con una mera sottovalutazione del canale comunicativo[127]. Al contrario, è proprio la loro particolare "ontologia" che sembra rendere i social media un luogo cospicuamente favorevole allo sviluppo di comportamenti impropri da parte del magistrato: come si è efficacemente sottolineato, è il design dei social media che pare "premiare" comportamenti disinvolti, ai limiti dell'istrionico, con maggiori *followers* e interazioni[128]. La dottrina statunitense riconduce questa peculiare capacità di determinare illeciti disciplinari a plurimi fattori: insieme all'effetto disinibitorio[129], la potenziale anonimità[130] e la viralità delle interazioni[131] contribuiscono a fare dei social media un «*ethical minefiled*» della responsabilità del giudice[132], senza peraltro dimenticare la loro capacità di fungere da cassa di risonanza per illeciti disciplinari compiuti fuori dal mondo virtuale[133]. A ciò si aggiunge la difficoltà, al fondo, di "interpretare" nel modo corretto le relazioni instaurate su tali mezzi di comunicazione[134]. Questo diffuso convincimento della letteratura statunitense sull'u-

[125] Diversi erano infatti gli avvisi all'inizio della riflessione: cfr. A. O'Brien, *The Judicial Process. Law, Courts, and Judicial Politics,* cit., 512.

[126] *«[T]here seems to be something about social media that is a multiplier for misconduct, perhaps the "online disinhibition effect" that has been identified for users in general. Moreover, given the high standards to which they are held, the ease of communication on social media poses particular dangers for judges by "encourag[ing] informality", "foster[ing] an illusory sense of privacy", and "enabl[ing] too-hasty communications that, once posted, are surprisingly permanent". […] The gratification that comes with others' "likes", "shares", and LOL comments can tempt judges to aim for attention-grabbing, rather than confidence-building, posts*» (C. Gray, *Stumbling Online*, in *Judges' Journal*, 3, 2019, 25–26).

[127] «[T]*he problem of unprofessional conduct online does not arise merely from a lack of appreciating the risks and hearing about the fallout*» (A. McPeak, *The Internet Made Me Do It. Reconciling Social Media and Professional Norms for Lawyers, Judges, and Law Professors*, in *Idaho Law Review*, 2, 2019, 206).

[128] «*It is more fundamentally a disconnect between the norms of online conduct and the real-world standards of professionalism. Social media platforms encourage oversharing and disinhibition. Their very design steers users to communicate in ways that deviate from real-world behavior. The community of users on a social media platform create their own social norms that steer the behavior of others in the online group. At the same time, legal professionals are held to a higher standard, often steeped in tradition. Lawyers, judges, and law professors are bound by ethics rules, workplace policies, or, more broadly, uncodified professional norms. Unfortunately, social media norms and professional norms often clash with each other, resulting in two competing sets of expectations and influences*» (*ibidem*).

[129] V. ivi, 212–213.

[130] V. ivi, 219–224.

[131] V. M.S. Kurita, Electronic Social Media. Friend or Foe for Judges, cit., 191–210, 223, 235.

[132] J.G. Browning, *Why Can't We Be Friends?*, cit., 533.

[133] Di questo «*social media effect*», che colpirebbe i giudici stessi ancor prima della fiducia pubblica nell'apparato giudiziario, parla diffusamente M.D. Goodman, *Shame, Angry Judges, and the Social Media Effect*, in *Catholic University Law Review*, 3, 2014, 608–613.

[134] «*Social media presents complex challenges for judges and the legal community at large because the personal relationships displayed through social media are often complex and easily misinterpreted*» (C. Estlinbaum, *Social Networking and Judicial Ethics*, in *St. Mary's Journal on Legal Malpractice and Ethics,* cit., 6).

nicità "di registro" dei social media sembra del resto trovare piena conferma nei primi commenti dell'area europea[135].

Detto di questo dato generale si può allora dare spazio dall'enucleazione dei nodi fondamentali della questione per come concettualizzati nella cospicua letteratura americana. Premettendo che più avanti, in sede di discussione comparatistica, si commenteranno alcuni "ulteriori interessi" in forza di cui parte della dottrina statunitense auspica una più forte presenza del giudice nella socialità virtuale, sembra qua innanzitutto opportuno capire quali criticità — più che quali opportunità — siano state associate all'utilizzo dei social media da parte dei magistrati. Del resto, questa sembra la prospettiva più corretta se si parte dal presupposto per cui in capo al giudice deve presumersi il godimento di tutte le situazioni giuridiche soggettive ascrivibili al cittadino ordinario, con conseguente spostamento dell'onere di prova sulle ragioni che giustificano eventuali limitazioni alle sue libertà in forza della particolarissima funzione esercitata.

2.4.1. I legami personali virtuali

I rischi per la percezione di imparzialità del giudice in una specifica vicenda giurisdizionale, derivanti dalla facilità con cui si instaurano legami personali via social media, hanno costituito il primo nodo problematico discusso dalla dottrina statunitense. Per lungo tempo, come si è potuto osservare, uno specifico frangente giuridico-tecnologico ha catalizzato l'attenzione delle autorità disciplinari e, per conseguenza, della dottrina: l'amicizia su Facebook tra il giudice e l'avvocato della stessa giurisdizione[136]. Tuttavia il punto rimane più generale, inerendo al significato da attribuire al legame

[135] Cfr. la *CGUE Opinion 25/2022*, cit., 16, che parla di «*specific risks» relativi ai social media: «The use of social media raises new challenges and ethical concerns relating to the propriety of the content posted and the demonstration of bias or interest. Social media features a broad accessibility and transmission, which entails greater scrutiny of the content posted. Social media has a permanent storage capacity, which enhances the risk of profiling. It contains personal communication in written form, which increases the risk of private messages being published without permission, as well as the risk of content being distorted in ensuing communication. Communication is fast and pointed, which might induce judges to publish imprudent posts. Actions, such as "liking" or forwarding information presented by others, may appear relatively small and casual, but they qualify as regular expressions of a judge's opinion. As opposed to traditional media, a gatekeeper is missing in social media, which allows judges to publish anything that comes to their mind*».

[136] Cfr. J.J. Alfini, *Future Trends in Judicial Ethics. The Influence of Cyberspace*, in *South Texas Law Review*, 4, 2010, 858–859; A. O'Brien, *The Judicial Process. Law, Courts, and Judicial Politics,* cit., 517–518; K.E. Vinson, *The Blurred Boundaries of Social Networking in the Legal Field. Just Face It*, in *University of Memphis Law Review*, 2, 2010, 401–402; S.V. Jones, *Judges, Friends, and Facebook. The Ethics of Prohibition*, in *Georgetown Journal of Legal Ethics,* cit., 288–301; T. Spahn, *The Rise of Facebook Creates Ethics Issues for Lawyers and Judges Ethics*, in *Experience*, 3, 2011, 36; C. Estlinbaum, *Social Networking and Judicial Ethics*, in *St. Mary's Journal on Legal Malpractice and Ethics,* cit., 12–15; B. Hull, *Why Can't We Be «Friends»? A Call for a Less Stringent Policy for Judges Using Online Social Networking*, cit., 609–616; N.J. Mitchell, *Judge 2.0. A New Approach to Judicial Ethics in the Age of Social Media,* cit., 2130–2138; D. Smith, *When Everyone is the Judge's Pal. Facebook Friendship and the Appearance of Impropriety Standard,* cit., 2–3; A.J. Wilson, *Let's Be Cautious Friends. The Ethical Implications of Social Networking for Members of the Judiciary*, in *Washington Journal of Law, Technology & Arts*, 3, 2012, 231–233; N.A. Boothe-Perry, *Friends of Justice. Does Social Media Impact the Public Perception of the Justice System*, in *Pace Law Review*, 1, 2014, 89–92; J.G. Browning, *Why Can't We Be Friends?*, cit., 491–496; B.P. Cooper, *Judges and Social Media. Friends with Costs and Benefits*, in *Professional Lawyer*, 3, 2014, 27–28; B.P. Cooper, *USA. Saving Face—Ethical Considerations for American Judges Using Facebook*, in *Legal Ethics*, 1, 2014, 150–152.

formale, sul social media, tra giudice e altro soggetto nel contesto di una valutazione dell'apparenza di imparzialità. Muovendo dal presupposto per cui il giudice che presieda una causa in cui è parte un proprio amico è senz'altro tacciabile di dubbi quanto alla sua imparzialità, al punto che tale situazione è generalmente proscritta dalle norme di procedura, viene naturale chiedersi se medesime considerazioni non debbano farsi in riferimento ad un «Facebook friend»[137]. E lo stesso può dirsi per lo status di follower su Twitter o per una *connection* su Linkedin: il filo rosso che lega tutti questi diversi frangenti è la «special position to influence the judge» in cui si troverebbe l'amico o il *follower*, qualsiasi sia poi, nei fatti, l'effettività di tale apparenza[138].

2.4.2. Le violazioni procedurali

Il secondo plesso problematico è costituito dalle insidie che i sociali social media "tendono" al regolare svolgimento del processo giurisdizionale, inteso come «*due process of law*»[139]. In primo luogo, i social media possono essere utilizzati per illegittime comunicazioni tra una delle parti e il giudice *absente altera parte* — le c.d. «*ex parte communications*»[140], che costituiscono una lesione manifesta al principio del contraddittorio[141]. In secondo luogo, i social media possono diventare un canale attraverso cui il giudice inviene di sua iniziativa fatti o indizi relativi alla personalità e alle vicende di vita delle parti o di altri soggetti rilevanti per il processo: di per sé illegittima in quanto incompatibile con il sistema accusatorio[142], questa attività di «ricerca indipendente» (*independent research*) trova nei social media un canale di diffusione tanto potente quanto difficilmente controllabile[143]. In terzo luogo, infine, appare in contrasto con il corretto dipanarsi della vicenda

[137] D. Smith, *When Everyone is the Judge's Pal. Facebook Friendship and the Appearance of Impropriety Standard,* cit., 2.

[138] «[A]*lthough social media friendship between a judge and a lawyer does not in fact mean that the lawyer is in a special position to influence the judge, it does convey that impression, thus violating the Code of Judicial Conduct*» (B.P. Cooper, *Judges and Social Media*, cit., 31).

[139] Cfr. D. Hricik, *Bringing a World of Light to Technology and Judicial Ethics*, in *Regent University Law Review*, 1, 2014, 20; M.S. Kurita, *Electronic Social Media. Friend or Foe for Judges,* cit., 217; E. Thornburg, *Twitter and the #So-CalledJudge,* cit., 307.

[140] La «*ex parte communication*» è definita come una «communication between counsel or a party and the court when opposing counsel or party is not present» (B. A. Garner (a cura di), *Black's Law Dictionary*, St. Paul, 2009, 316).

[141] «*These ex parte communications give the appearance that one side is in a position of influence; the potential for online ex parte communications which manifest such influence is one of the main reasons that the prohibitive advisory opinions restrict electronic social communications by judges*» (M.S. Kurita, *Electronic Social Media. Friend or Foe for Judges,* cit., 214).

[142] V. C.A. Dubay, *Public Confidence in the Courts in the Internet Age. The Ethical Landscape for Judges in the Post-Watergate Era*, in *Campbell Law Review*, 2, 2018, 535: «[W]*hile the digital frontier has offered exceptional opportunities for access to information on the Internet, judges continue to be bound by the strictures of the adversarial system that prohibit judges from conducting their own research on disputed factual issues*».

[143] «*Internet research of facts, like all forms of independent factual research by judges, is considered a form of ex parte communication because it occurs outside the presence of the parties and without an opportunity to cross-examine or object to its use.* […] *With respect to the core value of impartiality, the curious judge may wish to Google a party or find background information only to stumble upon unfavorable information that could explicitly or implicitly prejudice the judge towards a litigant or lawyer. Similarly, a judge may develop strong opinions or conclusions on disputed factual issues germane to the case when researching "background" information regarding an issue presented to the court for adjudication*»

processuale il comportamento del magistrato che sui social media faccia osservazioni e commenti sul processo in corso di svolgimento: nel momento in cui la Rule 2.10 del modello ABA — e sulla falsariga tutti i codici disciplinari statali — vieta qualsiasi esternazione del giudice «ragionevolmente» in grado di influenzare un processo in corso ovvero che in qualsiasi altro modo interferisca con il corretto espletamento di un giudizio pendente, simili commenti del magistrato sui social media sembrano senz'altro integrare i presupposti della violazione disciplinare[144].

2.4.3. Politicizzazione e personalizzazione della funzione giurisdizionale

Mentre nelle situazioni richiamate il problema è l'incidenza dei social media sull'integrità di un processo già instaurato, non meno preoccupante è il rischio di una lesione al corretto svolgimento di vicende giurisdizionali future o potenziali. L'ultimo nodo problematico — nonché la vera «crux of ethical worries about judicial involvement with social media»[145] — concerne il rischio che l'attività sui social media finisca per ledere la percezione di imparzialità del magistrato e, per l'effetto, la fiducia pubblica nella corretta amministrazione della funzione giurisdizionale: in questo caso l'imparzialità non è minacciata dalla creazione di specifici legami virtuali[146] — amicizie su Facebook, *following status* su Twitter, *connections* su Linkedin, etc. — quanto per la cospicua capacità dei social media di disvelare le inclinazioni etico-politiche dell'utente e dunque prospettivamente infirmare, *pro futuro,* l'apparenza di imparzialità del giudice quando questi sarà chiamato a decidere casi della vita in cui tali posizioni personali potrebbero mostrarsi in tensione con l'obiettività di giudizio. Il rischio, in altre parole, è quello di una "personalizzazione ideologica" — che eventualmente può assumere anche le forme di una vera e propria "politicizzazione" — della figura del magistrato.
Ben si coglie l'entità del problema in riferimento all'attività "comiziale" (*campaign speech*) degli aspiranti giudici chiamati a primeggiare in elezioni competitive con altri candidati. Alla luce di un generalizzato disinteresse per le elezioni dei giudici presso la popolazione, l'associazione del candidato con una determinata *Weltanschauung* ideologica — si pensi alla classica distinzione tra "conservatori" e "progressisti" — può fungere da catalizzatore del consenso elettorale. Al tempo stesso, è evidente il rischio che — specie in un contesto bipartitico come quello americano, sempre più «caratterizzato da una fortissima polarizzazione politica»[147] — l'attivismo "valoriale" del candidato sui social media possa portare alla sua ascrizione ad un determinato campo politico e per l'ef-

(*ibidem*).

144 A.J. Wilson, *Let's Be Cautious Friends. The Ethical Implications of Social Networking for Members of the Judiciary,* cit., 230. Cfr. ad es. il caso del giudice dello Stato del Minnesota Edward Bearse in J.G. Browning, *Should Judges Have a Duty of Tech Competence?*, cit., 181–182.

145 E. Thornburg, *Twitter and the #So-CalledJudge,* cit., 277.

146 Come pure può essere il caso: si v. la vicenda del giudice Steve Burgess che era chiamato a pronunciarsi sul rispetto dell'obbligo di registrazione di un lobbista repubblicano di cui il magistrato era *follower* su Twitter (cfr. J.G. Browning, *Judged by the (Digital) Company You Keep*, cit., 243–245).

147 F. Clementi, *La perdurante sfida del diritto al voto negli Stati Uniti*, in *Nomos*, 2, 2022, 2.

fetto ingenerare sospetti sulla sua effettiva imparzialità qualora questi, una volta eletto, si troverà a dirimere questioni giuridicamente e politicamente controverse. Del resto, anche quegli Stati che, come il Texas, arrivano ad ammettere l'esplicitazione dell'affiliazione partitica da parte del candidato categoricamente vietano l'esternazione di commenti capaci di prefigurare il suo futuro approccio giurisprudenziale a determinate tipologie di casi — le c.d. *commit clause*. Inevitabilmente finisce così per ingenerarsi una notevole tensione tra il divieto di pronunciarsi su questioni *lato sensu* politiche e la forma competitivo-elettorale del reclutamento dei magistrati[148]: non a caso questo dissidio ha dato luogo a note pronunce di legittimità costituzionale[149].

Se la regolamentazione dell'attività politica del candidato giudice varia in ragione delle diverse modalità di reclutamento negli Stati, molto più uniforme è invece il divieto di attività *lato sensu* politica da parte del giudice costituito[150], rispetto a cui forte è il timore che il summenzionato effetto "disinibitorio" dei social media porti alla compromissione dell'immagine di terzietà e imparzialità del giudice[151]. La preoccupazione, in altre parole, è che la visibilità e la viralità di interazioni "sospette" sui social media alimenti lo spettro di una «politicizzazione» — reale o soltanto percepita — dell'autorità giurisdizionale[152]. E poca differenza fa, al riguardo, che il sospetto tralucente dall'attività del magistrato sui social media sia quello di pregiudizio esplicitamente partitico o più generalmente ideologico-politico[153], quanto non di avversione rispetto ad un determinato genere[154] o ad una etnia[155], ovvero ancora verso un determinato organo istituzionale[156].

3. Una riflessione comparata sugli interessi di rilievo costituzionale

Come accennato in sede d'introduzione, obiettivo delle seguenti riflessioni comparate

148 «*There is — at least at first blush — something unseemly about nonpartisan interpreters of the law campaigning in much the same way as candidates running for a legislative or executive office*» (cfr. S.L.A. Dillard - B.M. McCormack, *The Robed Tweeter. Two Judges' Views on Public Engagement,* cit., 179).

149 Cfr. *Republican Party of Minnesota v. White*, 536 U.S. 765 (2002), in cui la Corte Suprema, con una *majority opinion* di Scalia, affermò l'incompatibilità di una *announce clause* — che vietava al candidato giudice di "dichiarare" la propria visione su «*disputed legal or political issues*» (ivi, 765) — con la libertà di manifestazione del pensiero di cui al First Amendment della Costituzione federale, seppur sostenendo di non «*assert nor imply that the First Amendment requires campaigns for judicial office to sound the same as those for legislative office*» (ivi, 783).

150 V. ad es. E. Thornburg, *Twitter and the #So-CalledJudge,* cit., 278–279.

151 V. nello stesso senso P. Sammarco, Giustizia e social media, cit., 122: «Se poi nel mondo reale il giudice è assai più cauto nel lasciarsi andare a frequentazioni personali e concedere a terzi la propria amicizia, nel mondo dei social network può capitare che taluno allenti i propri freni inibitori e allarghi le proprie maglie mostrando delle disponibilità inattese».

152 Cfr. *ex plurimis* E. Thornburg, *Twitter and the #So-CalledJudge,* cit., 292.

153 Si v. i casi "Kopf" (ivi, 282) e "Burgess" (su cui v. *supra* nota 146).

154 V. il caso "Kozinski" in J.J. Alfini, *Future Trends in Judicial Ethics. The Influence of Cyberspace,* cit., 861.

155 Si v. il caso "Olu Stevens" in J.G. Browning, *The Judge as Digital Citizen*, cit., 137–143.

156 Si v. il caso del profilo MySpace di un giudice del Nevada che esprimeva «a bias against prosecutors» in B. Hull, *Why Can't We Be «Friends»? A Call for a Less Stringent Policy for Judges Using Online Social Networking,* cit., 603.

sull'esperienza italiana non è quello di avanzare una specifica proposta normativa sulla risoluzione dell'intricato problema dell'utilizzo dei social media da parte dei magistrati. Certo, l'analisi di diritto comparato sembrerebbe aver già messo in fuorigioco la desiderabilità di soluzioni «draconiane»: da una parte, benché una pluralità di ragioni potrebbe rendere l'astensione dai social media l'opzione più saggia per il magistrato — come sua scelta personale — sembra affatto ingiustificata la determinazione potestativa di un simile esito mediante espresso divieto; d'altra parte, il novero delle problematiche rilevate nell'esperienza statunitense dovrebbe aver altresì reso inverosimile la prospettiva di una semplice *deregulation*. E nemmeno granché risolutiva pare, inoltre, l'idea di ammettere un utilizzo dei social media per i soli profili attinenti alla vita privata del giudice, atteso che non solo una simile soluzione non risponde ad alcune problematiche — si pensi alla *vexata quaestio* dei legami virtuali tra giudice e avvocato, che ben potrebbero aver sviluppato una qualche forma di legittima "amicizia" in ragione del comune percorso universitario — ma anche poiché le stesse vicissitudini della vita privata si riverberano, nel caso del giudice, sulla sua attività professionale[157].

Piuttosto che una vera e propria proposta di intervento normativo, si intende qui riflettere su un profilo che dovrebbero apparire attuale qualsiasi corso — più o meno restrittivo — dovesse essere intrapreso dal legislatore italiano nella sua discrezionalità, ovvero da altra "competente autorità normativa". Informati alla paradigmatica esperienza statunitense, ci si propone di mettere a fuoco gli interessi di rilievo costituzionale che sembrano venire in rilievo davanti alla questione di politica del diritto. In particolare, si traccerà qui una linea rossa tra due ricostruzioni del problema, a seconda dei diversi interessi ritenuti considerabili dal legislatore. Nella prima "classica" ricostruzione, al generale interesse al godimento da parte del magistrato della libertà di espressione a lui riconosciuta *uti civis* si contrappone il controinteresse all'imparzialità e indipendenza della magistratura e, per l'effetto, all'integrità del processo giurisdizionale. Nella seconda ricostruzione, al contrario, altri "ulteriori interessi" devono entrare nel bilanciamento legislativo, inevitabilmente adombrando una regolamentazione più lasca — se non per certi versi *esortativa* — dell'utilizzo dei social media da parte dei magistrati. Pur prendendo posizione a favore dell'approccio "classico" e dunque verosimilmente più restrittivo, ciò che si vuole qui soprattutto enfatizzare è il nesso tra la scelta degli interessi che si ritengono partecipanti al bilanciamento legislativo e una più generale concezione della magistratura nello Stato costituzionale di diritto.

[157] Come molto chiaramente rileva A. McPeak, *The Internet Made Me Do It. Reconciling Social Media and Professional Norms for Lawyers, Judges, and Law Professors,* cit., 226: «*One solution to the challenges of social media professionalism is to maintain separate accounts for personal and professional tweets. But for many legal professionals, one's career identity may be difficult to separate from one's personal life. Additionally, divorcing real-world and online personas can be messy and fraught with error. And even seemingly innocuous attempts to separate real-world and online personas still create the risk of disinhibited behavior and unprofessionalism. For example, some professionals prefer to treat social media as only a personal tool. But even personal accounts must conform with professional norms. One purpose of professional norms is to present to the public a dignified image of the profession, whether it be lawyers, judges, or law professors. Inappropriate content on a personal account still leaves a bad impression on members of the public who have access to the personal account contents. Further, a user's social media networks inevitably begin to blend professional and personal contacts, so that it becomes impossible to isolate one's personal life from the professional one*».

3.1. La "contrapposizione tradizionale"

Nella regolamentazione dell'uso dei social media da parte dei magistrati e nella letteratura a commento costantemente ritorna una contrapposizione tra interessi di rilievo costituzionale che, per la frequenza con cui viene invocata e nei sistemi di *common law* e in quelli di *civil law*, può certamente presentarsi come la «contrapposizione tradizionale» nella materia *de qua*: mentre ad un angolo starebbe la tutela dei diritti di libertà di cui il magistrato gode *uti civis* — venendo qui in speciale rilievo il diritto alla libera manifestazione del pensiero e il diritto di associazione — all'altro angolo vi sarebbe l'interesse all'imparzialità — se non altro nella forma dell'*immagine di imparzialità* — nell'amministrazione della giustizia, che in certi casi e a determinate condizioni giustificherebbe la compressione delle libertà costituzionali del cittadino-giudice[158]: sul legislatore cadrebbe dunque il compito di una valutazione comparativa degli interessi, al fine di un bilanciamento che, benché in parte discrezionale in quanto espressione di variabili sensibilità politiche, in alcune giurisdizioni incontra un limite nel sindacato di ragionevolezza del giudice costituzionale. Si tratta, beninteso, di una contrapposizione che in radice evidentemente trascende i social media: da una parte, in altri noti frangenti la libertà di associazione del giudice è stata sottoposta a limiti[159]; dall'altra, il problema del bilanciamento tra diritti del magistrato *uti civis* e tutela dell'imparzialità della funzione giurisdizionale si è storicamente espanso anche ad altre libertà costituzionali, come chiaramente dimostra la portata transnazionale del dibattito sull'esercizio del diritto di sciopero da parte dei magistrati[160].

L'ubiquitaria presenza della contrapposizione tradizionale nelle fonti di *civil law* e *common law* attesta, innanzitutto, la convergenza delle aspettative sociali verso l'esercizio

---

158 Cfr. Cal. Judges Ass'n Jud. Ethics Comm., Opinion 66, cit., 5 («*Judges must be careful to avoid making remarks that would cast doubt on the judge's ability to act impartially*»); Cal. Sup. Ct. Comm. Jud. Ethics, Expedited Opinion 2021–042, cit., 5 («*When posting comments online, judges must carefully consider the canons and the potential hazards of social media to strike a balance between the restrictions on judicial conduct and the expression of personal opinions*»); N.M. Advisory Comm. C. Jud. Conduct, Opinion 2016, cit.: («*it would be inappropriate for the judge to express an opinion that may have bearing on the judge's impartiality or fairness*»); ABA, Formal Opinion 462, cit., 1–2 («*Comments, images, or profile information, some of which might prove embarrassing if publicly revealed, may be electronically transmitted without the judge's knowledge or permission to persons unknown to the judge or to other unintended recipients. Such dissemination has the potential to compromise or appear to compromise the independence, integrity, and impartiality of the judge, as well as to undermine public confidence in the judiciary*»); Okla. Jud. Ethics Advisory Panel, Opinion 2011–3, cit., § 6–9 («*The common theme of the opinions rendered in other states deals with the conflict that may arise between the use of the social network and the duty of the Judge, found in all the Codes of Judicial Conduct, that is the duty of the Judge to maintain the dignity of judicial office at all times, and avoid impropriety and the appearance of impropriety in their professional and personal lives, and to ensure the greatest public confidence in their independence, impartiality, integrity and competence.* […] *We believe that public trust in the impartiality and fairness of the judicial system is so important that is imperative to err on the side of caution where the situation is "fraught with peril"*»); N.Y. St. Advisory Comm. Jud. Ethics, Opinion 11–125, cit. («*a judge must not allow family, social, political or other relationships to influence the judge's judicial conduct or judgment* […] *and must disqualify him/herself in a proceeding in which the judge's impartiality might reasonably be questioned*»). Nella dottrina *ex plurimis* v. E. Thornburg, *Twitter and the #So-CalledJudge,* cit., 294–298.

159 Si pensi al divieto di iscrizione ai partiti politici (su cui *ex plurimis* v. G. Ferri, *La magistratura in Italia,* cit., 249 ss.) sia al divieto di partecipazione ad associazioni segrete (su cui *ex plurimis* v. F. Biondi, *La responsabilità del magistrato. Saggio di diritto costituzionale*, Milano, 2006, 304–308).

160 Sul tema si permette il rimando a S.R. Vinceti, *Sciopero dei magistrati e costituzioni. L'esperienza italiana in prospettiva comparata*, Roma, 2023.

della funzione magistratuale nelle due grandi famiglie della tradizione giuridica occidentale[161]. Al netto dunque delle innegabili differenze che possono intercorrere — dal punto di vista del reclutamento, della forma di governo, della partecipazione del popolo all'esercizio della giustizia, del ruolo del precedente, etc. — l'analisi qui condotta segna un punto a favore dell'unitarietà della concezione della magistratura nella *western legal tradition*[162], sconfessando, in certo qual modo, visioni antinomiche che enfatizzando a dismisura le peculiarità sancirebbero la sostanziale incomparabilità del giudice di *common law* e di *civil law* pur nel comune contesto dello Stato costituzionale di diritto. Al contrario, proprio il fatto che anche gli ordinamenti giudiziari statunitensi, cospicuamente caratterizzati da forme di elettività assimilabili a quelle previste per gli organi rappresentativi nei Paesi di *civil law*, cerchino con forza di escludere ogni possibile "debordamento politico" della figura del giudice — tale da potere minare l'imparzialità dell'amministrazione della giustizia — conferma[163] — anche nel contesto di un fenomeno nuovo e per plurimi versi irriducibile come i social media — la comune visione del potere giudiziario nello Stato costituzionale di diritto e, in esso, l'attualità

[161] Sull'avvento del costituzionalismo come elemento unificatore delle esperienze occidentali v. G. Bognetti, *Introduzione al diritto costituzionale comparato. (Il metodo)*, Torino, 1994, 79. Sul punto cfr. altresì A. Gambaro - R. Sacco, *Sistemi giuridici comparati*, Milano, 2018, 36–38, e G.F. Ferrari, *«Civil law» e «common law». Aspetti pubblicistici*, in P. Carrozza - A.D. Giovine - G.F. Ferrari (a cura di), *Diritto costituzionale comparato*, vol. II, Roma-Bari, 2014, 788–793. Sull'aumento della creatività della giurisprudenza come fattore del «potente movimento di avvicinamento reciproco fra le due grandi famiglie giuridiche» v. M. Cappelletti, *Giudici legislatori*, cit., spec. 110–115.

[162] La letteratura sulla fisionomia della funzione magistratuale nelle famiglie di *civil law* e *common law* è evidentemente vasta. Limitando l'ambito di indagine alle trattazioni generali della letteratura italiana cfr. M. Cappelletti, *Giudici legislatori?*, Milano, 1984, spec. 100–110; A. Pizzorusso, *Sistemi giuridici comparati,* cit., spec. 215–242; U. Mattei, *Il modello di common law*, Torino, 2014, spec. 22–23, 85–88, 138–140; M. Mazza, *Il potere giudiziario*, in P. Carrozza - A. Di Giovine - G.F. Ferrari (a cura di), *Diritto costituzionale comparato*, vol. II, Roma-Bari, 2014, spec. 1069–1074; A. Somma - P.G. Monateri, *Il modello di civil law*, Torino, 2016, spec. 123–124, 167–168; L. Pegoraro - A. Rinella, *Sistemi costituzionali comparati*, Torino, 2017, 518–524; V. Varano - V. Barsotti, *La tradizione giuridica occidentale,* cit., spec. 171–179, 269–289, 323–336. Ancora vivide risultano peraltro le pagine di L.J. Constantinesco, *Traité de Droit Comparé. Tome III (La science des droits compares)*, Paris, 1983, 374–377, e J.H. Merryman - R. Pérez-Perdomo, *The Civil Law Tradition. An Introduction to the Legal Systems of Europe and Latin America*, Stanford, 2007, spec. 34–38, cui può ovviamente aggiungersi R. David - C. Jauffret-Spinosi, *Les grands systèmes de droit contemporains*, Paris, 1982, 132 ss..

[163] Che da un punto di vista comparatistico l'elettività del giudice non comporti affatto la sua "politicizzazione" corrobora le risultanze dell'indagine storico-giuridica: «[Q]uesto modo [elettivo] di provvedere alla formazione dell'ordine giudiziario […] è, oltre tutto, un modo arcaico di scegliere gli "operatori di giustizia", e pur nel Medioevo comunale, quando ardeva la lotta delle fazioni nelle nostre città, si cercò di sottrarre la loro scelta al giuoco dei contrasti politici e i giudici venivano estratti da appositi elenchi (o matricole o mariegole), nel quale potevano essere iscritti soltanto coloro che avevano studiato in uno *studium generale* per un certo numero di anni, anche se non avevano conseguito il titolo dottorale, e codesta estrazione aveva luogo secondo l'ordine di iscrizione nell'elenco. E l'elezione dei giudici si venne dovunque dove prima dove dopo spegnendo: il giudice "dotto", che prende il posto del giudice popolare, non tollera il sistema di una scelta abbandonata alle lotte delle forze politiche. *Ad ogni modo, anche dove e quando l'elezione fu adoperata, non significò mai che il giudice dovesse applicare il diritto secondo parametri politici o, peggio ancora, per ottenere una trasformazione della società, ma per applicare la legge senza paura e senza odio "sola facti veritate inspecta"*; ed era astretto a ciò da un giuramento solenne e, uscito che fosse di carica, era soggetto al "sindacato", un processo celebrato davanti ad un giudice quasi sempre "estraneo" alla città, davanti al quale coloro che lamentavano di aver sofferto un'ingiustizia, proponevano la loro azione e il giudice non poteva abbandonare la città prima che questo processo fosse celebrato» (G. Cassandro, *I giudici elettivi*, in *Dir. soc.*, 1, 1978, 163–164 (corsivo aggiunto)).

epistemologica della distinzione tra *gubernaculum* e *iurisdictio*[164], tra *law-creation* e *law-application*[165], oltre che la connessa «cesura istituzionale» tra ordine giudiziario e circuito politico-rappresentativo[166].

Al tempo stesso, nella discussione sulla regolamentazione dell'uso dei social media da parte dei magistrati si osserva altresì l'emersione di alcuni "ulteriori interessi" che secondo alcune voci della dottrina — spesso giudici a loro volta — e di alcune autorità normative dovrebbero essere contemplati nel bilanciamento tra degli interessi da parte del competente *policymaker* e che, interessantemente, non sembrano riconducibili alla descritta «contrapposizione tradizionale». In queste ricostruzioni, i mezzi elettronici di comunicazione sociale sono valorizzati al fine di conseguire, in particolare, due risultati: (i) un maggiore coinvolgimento della magistratura con la propria comunità di riferimento, che può prendere le forme di una vera e propria (ii) attività "educativa" dei cittadini da parte dei magistrati sull'organizzazione giudiziaria e il diritto stesso. Al commento di questi "ulteriori interessi" e al nesso con la discussione della posizione del potere giudiziario nello Stato costituzionale di diritto sono dedicate le sezioni che seguono.

3.2. Gli "ulteriori interessi"

3.2.1. Il coinvolgimento sociale

Il primo "ulteriore interesse" per cui dovrebbe incoraggiarsi l'utilizzo dei social media da parte dei magistrati è il conseguimento di un maggiore coinvolgimento del giudice con la comunità in cui è chiamato a svolgere la propria funzione. Il punto di partenza è il dato di una storica "distanza umana" tra il magistrato e i cittadini: laddove altri funzionari pubblici mantengono infatti un legame vivo e diretto con la popolazione per tutta la durata della carica, l'apoliticità della funzione giurisdizionale avrebbe storicamente allontanato il giudice dalla propria comunità di riferimento e dalle sue aspettative[167]. Chiusi nelle loro «*ivory tower[s]*»[168] i giudici sarebbero criticabili «for being

[164] Cfr. C.H. McIlwain, *Constitutionalism, Ancient and Modern*, Ithaca, 1947, 67 ss.

[165] Cfr. H. Kelsen, *General Theory of Law and State*, Cambridge, 1949, 255–260. Per una recente difesa della distinzione — contro la stessa relativizzazione kelseniana (ivi, 269–270) — cfr. P. Sandro, *The Making of Constitutional Democracy. From Creation to Application of Law*, New York, 2022.

[166] «L'inesistenza di una "linea di continuità" caratterizza invece i rapporti tra giudici e legislatori nell'attuazione dello Stato costituzionale di diritto. Lo Stato di diritto si fonda tradizionalmente su di una cesura istituzionale tra i due ordini. Poco importa qui approfondire la completa coerenza, nell'esperienza concreta, degli ordinamenti del passato a tale postulato teorico. Non vi è dubbio che le costituzioni contemporanee accolgono e si ispirano a tale principio di reciproca indipendenza». E. Gianfrancesco, *Il principio dello Stato di diritto e l'ordinamento europeo*, in S. Mangiameli (a cura di), *L'ordinamento europeo*, Milano, 2006, 267.

[167] «*For most of American history, the judge has been viewed as a different type of public servant. Unlike other public officials, judges are typically (and correctly) not considered politicians, and they are far less likely to interact with their constituents on a regular basis. Instead, they toil away in cloistered courthouses in relative anonymity, making decisions in civil and criminal matters of the utmost importance*» (S.L.A. Dillard - B.M. McCormack, *The Robed Tweeter. Two Judges' Views on Public Engagement,* cit., 179).

[168] P.M. Reyes Jr., *To Post Or Not to Post. Judges on Social Media,* cit., 21.

inaccessible and a source of mystery to the public they serve»[169]: da qui la loro frequente rappresentazione nei termini di oracoli anonimi e distaccati di un "freddo" diritto oggettivo, che applicherebbero con deliberata apatia nella solitudine delle proprie stanze[170]. Per i fautori di un maggiore coinvolgimento sociale del magistrato, questa situazione dovrebbe evidentemente cambiare, portando il giudice alla luce di un contatto diretto con le persone[171].

Da questo punto di vista, è evidente il potenziale dei social media come strumento per cambiare l'immagine di un apparato giudiziario secluso dalla propria comunità di riferimento[172]. Benché siano senz'altro prospettabili altre modalità di coinvolgimento con la "società civile" — si pensi alle occasioni di confronto universitario o alle attività culturali — la viralità e pervasività che rendono i social media così problematici[173] li rendono al tempo stesso idonei a rivoluzionare il *public engagement* del magistrato: le limitazioni spaziali e temporali che riducono l'impatto delle iniziative pubbliche di un giudice di per sé già assorbito dall'attività *stricto sensu* giudiziaria vengono infatti immediatamente meno nel mondo della socialità online[174]. In altre parole, è la tecnologia stessa dei social media, il suo «broad reach»[175], che legittimerebbe un ripensamento *ab imis* del ruolo del magistrato della società[176]. Laddove il sito istituzionale di un determinato tribunale raramente riporta le modalità con cui un determinato giudice è attivo nella società, al di fuori della sua funzione istituzionale[177], sui social media il magistrato può pubblicizzare direttamente questo materiale e, così facendo, sensibilizzare la comunità su simili iniziative[178].

---

169 J.G. Browning, *Why Can't We Be Friends?*, cit., 131.

170 «[T]*he imagery often associated with the judiciary is that of a wise but entirely detached body of individuals who sit on elevated benches, adorn themselves in majestic black robes (with gavels in hand), and dispassionately rule on the various and sundry disputes of the day (and do so largely out of the public eye)*» (S.L.A. Dillard, #*Engage. It's Time for Judges to Tweet, Like, & Share*, in *Judicature*, 1, 2017, 11).

171 «*In our view, it is long past time for judges to reimagine how they participate in their communities. They can (and we think should) engage and educate the people they serve on a regular basis. We judges need to […] step out of our courtrooms and into the light of day. We are public servants, not disengaged robed philosophers, and the public has a right to know who we are and what we do*» (S.L.A. Dillard - B.M. McCormack, *The Robed Tweeter,* cit., 180).

172 «[O]*ne of the best ways for judges to effectively engage the people they serve is to embrace the ubiquitous social-media platforms other citizens use to communicate and interact with one another*» (*ibidem*).

173 Cfr. *supra* § 2.4.

174 «[T]*he reality is that there are only so many events that a judge can attend, only so many hands that a judge can shake, and only so many hours in the day. After all, a judge does still have to perform his or her judicial duties, which are often extraordinarily difficult and time consuming*» (S.L.A. Dillard, #*Engaged,* cit., 12).

175 P.M. Reyes Jr., *To Post Or Not to Post. Judges on Social Media,* cit., 23.

176 «*This* […] *is where technology and social media can be of a tremendous benefit to the public. Indeed, the ability of a judge to use social media to directly reach and communicate with his or her constituents is nothing short of revolutionary*» (S.L.A. Dillard, #*Engaged,* cit.). Nello stesso senso S.L.A. Dillard - B.M. McCormack, *The Robed Tweeter,* cit., 182–183.

177 P.M. Reyes Jr., *To Post Or Not to Post. Judges on Social Media, et loc. ult.* cit.

178 *Ibidem*.

3.2.2. L'impegno educativo

Strettamente connesso al profilo del coinvolgimento sociale, ma dotato di un sufficiente grado di indipendenza concettuale da giustificarne una trattazione autonoma, è la dimensione dell'impegno educativo. Più che la separatezza del magistrato rispetto alla comunità di riferimento, quanto qui si vuole contrastare è la misteriosità che contorna l'organizzazione giudiziaria, il funzionamento dei processi e per certo versi il diritto *tout court*: nel momento in cui «[t]*he courts remain the most misunderstood and elusive branch of government*»[179], in quanto «*least known, understood, and publicized*»[180], e più in generale il diritto appare «*mysterious and a bit frightening to those who do not work in the legal profession*»[181], sui giudici ricadrebbe una «*affirmative responsibility […] to educate the public about the judicial institution and create an open and transparent understanding of the courts*»[182], che a sua volta rafforzerebbe la fiducia nell'integrità della giustizia[183].

Rispetto a questo ulteriore interesse, i social media appaiono «unique, cost-effective tools to engage and educate the public»[184] in quanto permettono di disseminare l'attività di educazione giuridica del giudice presso una parte ben più estesa, potenzialmente illimitata, della popolazione.[185]. E se in questo modo i giudici eletti hanno la possibilità di interagire direttamente con i propri elettori[186], anche gli altri sono chiamati ad usare i social media per analoghe attività educative[187]. Le forme concrete di questo "impegno educativo" sono descritte in prima persona da due vivaci sostenitori di un simile uso dei social media: dalla diffusione dei comunicati stampa delle Corti, all'istruzione sugli adempimenti burocratici e processuali, fino alla condivisione delle foto degli eventi sociali, ovvero di articoli o contributi dei magistrati su temi di interesse pubblico[188]. In quest'ottica, peraltro, dovrebbe guardarsi con sfavore qualsiasi preclusione sugli argomenti giuridici trattati dal giudice sui social media, anche laddove forieri di dissenso o divisione nell'uditorio[189].

---

179 M.S. Kurita, Electronic Social Media. Friend or Foe for Judges, cit., 198.

180 P.M. Reyes Jr., *To Post Or Not to Post. Judges on Social Media,* cit., 24.

181 S.L.A. Dillard, #*Engaged,* cit., 11.

182 M.S. Kurita, *Electronic Social Media. Friend or Foe for Judges,* cit., 198.

183 Cfr. J.G. Browning, *Judged by the (Digital) Company You Keep*, cit., 224. Nello stesso senso N.J. Mitchell, *Judge 2.0. A New Approach to Judicial Ethics in the Age of Social Media,* cit., 2137.

184 S.L.A. Dillard - B.M. McCormack, *The Robed Tweeter. Two Judges' Views on Public Engagement,* cit., 180.

185 «[O]*nline social networking allows the judge to reach a broader audience so the judge can help educate the public about the law*» (B. Hull, *Why Can't We Be «Friends»? A Call for a Less Stringent Policy for Judges Using Online Social Networking,* cit., 629).

186 A. McPeak, *The Internet Made Me Do It. Reconciling Social Media and Professional Norms for Lawyers, Judges, and Law Professors,* cit., 227.

187 S.L.A. Dillard - B.M. McCormack, *The Robed Tweeter. Two Judges' Views on Public Engagement,* cit., 185.

188 «*We provide links to press releases issued by our courts. We educate the public about our courts' deadlines and processes. We highlight job openings at our courts, and post photos and information about events we attend in our official capacities. We post links to our opinions, scholarly articles and essays, and other informative writings*» (*ibidem*).

189 «[D]*iscouraging any tweet that deals with legal topics that are part of the current debate, just because some might disagree with them, would greatly impoverish the judiciary's ability to contribute to civic education and the improvement of the legal system*» (E. Thornburg, *Twitter and the #So-CalledJudge,* cit., 307).

3.3. Verso una nuova identità costituzionale del magistrato?

Benché non esauriscano il catalogo delle finalità giustificatrici di una più forte presenza dei giudici sui social media[190], gli "ulteriori interessi" appena richiamati ben rappresentano il senso delle ragioni in base a cui una parte della magistratura statunitense — sulla scia di adombramenti di alcune autorità di *advisory* disciplinare[191] — ha incoraggiato l'uso dei social media da parte dei magistrati. Quello che qui si intende fare è lumeggiare il nesso tra la perorazione di questo maggiore coinvolgimento sociale del giudice — e dunque di una regolamentazione più aperturista, quando non effettivamente *esortativa*, dell'utilizzo dei social media da parte dei magistrati — e una rinnovata visione del ruolo della magistratura nello Stato costituzionale di diritto. Il fine, beninteso, non è criticare o financo banalizzare questa concezione — magari agitando lo spettro del "giudice influencer"[192] nello stesso modo in cui i detrattori della visione classica del potere giudiziario sventagliano la vituperata immagine montesqueiana del giudice "*bouche de la loi*" — quanto piuttosto sostenere, più pianamente, che la risoluzione della "settoriale" questione di politica del diritto — l'adozione di un approccio restrittivo o aperturista sull'uso dei social media da parte dei membri dell'ordine giudiziario — dipende in larga misura dalla posizione che si voglia assunta nel risalente e più fondamentale dibattito

[190] Dillard e McCommarck adombrano anche altre funzioni "accessorie" come ad es. il rafforzamento dei rapporti di colleganza e mutuo sostegno professionale, il tutoraggio degli studenti di diritto o dei tirocinanti, il miglioramento della conoscenza dei social media come fenomeno sociale, da parte del giudice, in una sorta di *learn by doing* (cfr. S.L.A. Dillard - B.M. McCormack, *The Robed Tweeter. Two Judges' Views on Public Engagement,* cit., 186–187). Thornburg contempla persino l'uso dei social media come strumento di resistenza politica: «*in this day and age, when much of America gets its news from social media and those platforms are being used to delegitimize the judiciary, the third branch can ill afford to disengage. Judicial tweeting, within the limits of the ethics rules, should be encouraged rather than shunned*» (E. Thornburg, Twitter and the #So-CalledJudge, cit., 253).

[191] Cfr. Cal. Sup. Ct. Comm. Jud. Ethics, Expedited Opinion 2021–042, cit.; Ky. Jud. Ethics. Comm., Opinion 2010–119, cit.

[192] Già illuminavano questo rischio le pagine polemiche di Marafioti, pur redatte prima dell'avvento dei social media: «Il giudice d'oggi, cambiato e sfigurato nei suoi tratti peculiari, appare piuttosto incline alle logiche di dominio e ai miti della cultura-spettacolo, prodotto deteriore della cosiddetta *societé du spectacle*. Donde le esaltazioni, nell'immaginario collettivo, di "giudici contro", in lotta contro l'ingiustizia, nel segno di Zorro, di togati che imperversano sulle pagine di quotidiani e periodici, nel clamore dell'intervista, ritratti a piedi o a cavallo, o in tenuta di calciatori, o che dismettono la toga davanti alle telecamere alla conclusione di uno "storico" processo; e via dicendo, nell'aria del tempo, dei riti circensi e delle velleità di protagonismo. Tutto il contrario del costume del riserbo e della natura dell'impegno che si richiedono e si addicono al mestiere del giudice» (D. Marafioti, *Metamorfosi del giudice. Riflessioni su giustizia e potere*, Soveria Mannelli, 2004, 17–18). Di recente, ha valutato con favore «la recente riforma dell'ordinamento giudiziario che, al fine di limitare il protagonismo di alcuni PM, ha vietato le esternazioni dei singoli sostituti nei rapporti con la stampa» V.M. Caferra, *La prospettiva del magistrato*, in G. Resta (a cura di), *Il problema dei processi mediatici nella prospettiva del diritto comparato* cit., 196, evidentemente reiterando il preoccupato giudizio sul fenomeno espresso a suo tempo (cfr. V.M. Caferra, *Il magistrato senza qualità*, Bari, 1996, 101: «Il protagonismo induce il magistrato ad entrare in rapporto diretto col mondo dell'informazione e ad acquisirne il linguaggio e le tecniche di comunicazione. Per ottenere il sostegno dell'opinione pubblica non può restare fuori del circuito della moderna comunicazione; perciò non rinunzia ad essere oggetto dell'attenzione dei media, quando non diventa egli stesso la fonte principale dell'informazione in materia giudiziaria»).

sulla collocazione della magistratura nello Stato costituzionale di diritto[193]: a riprova, se mai ve ne fosse stato il dubbio, dell'attualità del problema di teoria costituzionale, che può senz'altro dichiararsi irrisolto anche nell'era dei social media.

La «contrapposizione tradizionale» sopra richiamata si muove infatti nel solco di una visione classica secondo cui «*the function of the judiciary is to decide disputes in accordance with the law and with impartiality*»[194]. Per dirla con Blackstone, il giudice è non è chiamato a decider secondo «*his own private judgment», ma «according to the known laws and customs of the land*»: suo compito non è creare «*new law*», bensì «*to maintain and expound the old one*»[195]. In questa concezione, cifre della funzione magistratuale sono l'intellettualità e l'imparzialità — da intendersi qui in senso coestensivo con la nozione di "neutralità"[196]. Certo non scevra da esasperazioni — esemplificate da certe "visioni sacerdotali" del potere giudiziario[197] — la «traditional view» gode di una permanente significatività nella

[193] Su cui cfr. S. Gambino (a cura di), *La magistratura nello Stato costituzionale. Teoria ed esperienze a confronto*, Milano, 2004; S. Sicardi, *Percorsi e vicende del Terzo Potere dallo Stato liberale allo Stato costituzionale. Da uno sguardo d'insieme alla situazione italiana*, in Id. (a cura di), *Magistratura e democrazia italiana. Problemi e prospettive*, Napoli, 2010, 1 ss.; A. Di Giovine - A. Mastromarino, *Il potere giudiziario nella democrazia costituzionale*, in R. Toniatti - M. Magrassi (a cura di), *Magistratura, giurisdizione ed equilibri istituzionali. Dinamiche e confronti europei e comparati*, Milano, 2011, 17 ss.

[194] «*The law is thought of as an established body of principles which prescribes rights and duties. Impartiality means not merely an absence of personal bias or prejudice in the judge but also the exclusion of 'irrelevant' considerations such as his political or religious views*». Così efficacemente definisce la «traditional view» prima di sottoporla a critica — per certi versi un po' sommaria, ma certo rappresentativa — J.A.G. Griffith, *The Politics of the Judiciary* (1977), Glasgow, 1985, 193.

[195] W. Blackstone, *Commentaries on the Laws of England*, vol. I, Oxford, 2016, 52.

[196] Per questa accezione di "neutralità" v. *ex plurimis* M. Cappelletti, *La testimonianza della parte nel sistema dell'oralità. Contributo alla teoria della utilizzazione probatoria del sapere delle parti nel processo civile*, vol. I, Milano, 1962, 41; E. Amodio, *Estetica della giustizia penale. Prassi, media, fiction*, Milano, 2016, 57; C. Bologna, *Apparenza d'imparzialità tirannia dell'apparenza? Magistrati e manifestazione del pensiero*, in *Quad. cost.*, 3, 2018, 638; A. D'Aloia, *I Consigli di autogoverno delle magistrature speciali. Bilancio di un'esperienza e problemi (ancora) aperti*, in *Riv. trim. sc. amm.*, 2, 2021, 13; G. Scaccia, *L'etica della funzione giudiziaria. Fra teoria dell'interpretazione e separazione dei poteri*, in *Quad. cost.*, 2, 2023, spec. 467–470. Di "neutralità" parla del resto la stessa Corte cost.: cfr. sent. 26 febbraio 2014, n 39, *cons. in dir.* § 6.3.3; sent. 6 luglio 2000, n. 283, *cons. in dir.* § 3-4; sent. 29 settembre 1997, n. 306, *cons. in dir.* § 2.1. Peraltro, questa accezione di "imparzialità" è sovrapponibile alla nozione di «fedeltà» per come definita da G. Lombardi, voce *Fedeltà (dir. cost.)*, in *Enc. dir.*, XVII, Milano, 1968, 175 («un imperativo alla neutralità politica da parte dei titolari di pubblici uffici»). Preferiscono invece distinguere "imparzialità" e "neutralità" N. Zanon - F. Biondi, *Il sistema costituzionale della magistratura*, Bologna, 2019, spec. 191–193.

[197] Si v. ad es. G. Persico, *La nuova magistratura*, Roma, 1945, 46: «I magistrati dovranno considerare la loro missione come un vero e proprio sacerdozio, e conseguentemente non potranno iscriversi ad alcun partito politico, in quanto deve essere evitato, come per la moglie di Cesare, anche il più remoto e lontano sospetto sulla indipendenza ed imparzialità di esercizio della loro funzione». L'associazione tra ordine giudiziario e ordine sacerdotale è del resto presente anche nell'esperienza statunitense, pure informata ad una più netta separazione tra Stato e Chiesa. Si v. ad es. il significativo passaggio di Blue: «*The legal theme, frequently announced as a public article of faith by judges and politicians alike, is that the task of judging involves a faithful and learned adherence to the Law (with a capital "L"), without reference to the personal views of the judge. Due process, which requires "an impartial and disinterested tribunal", implicitly demands this fidelity. The psychological theme, rarely articulated but fervently believed by many members of the judiciary, is that, if public faith in the courts is to be maintained, the public must view the judges as a* priestly caste» (J.C. Blue, *A Well-Tuned Cymbal? Extrajudicial Political Activity*, in *Georgetown Journal of Legal Ethics*, 1, 2004, 14–15 (enfasi aggiunta)). Sull'immagine "sacerdotale" del giudice e sul tema della magistratura come «*secular papacy*» v. diffusamente G. Resta, *Il problema dei processi mediatici nella prospettiva del diritto comparato, cit.*, 8–11.

teoria costituzionale[198] come nell'esperienza comune: lo stesso cittadino, del resto, ne è subito avvertito alla vista dei "paramenti magistratuali", simbolo per eccellenza della "spersonalizzazione" del giudice in chiave di massima imparzialità[199]. All'interno della «*traditional view*» la ricerca dell'equilibrio *de iure condendo* in riferimento ai social media non può che svolgersi nel familiare perimetro del contemperamento dell'imparzialità dell'autorità giurisdizionale e della legittima aspettativa del cittadino-giudice a vedersi dimidiato solo di quelle frange di libertà al cui sacrificio possa aver ragionevolmente consentito con la scelta di entrare nell'ordine giudiziario.

Al contrario, gli "ulteriori interessi" al coinvolgimento sociale e all'impegno educativo — la cui tutela dovrebbe giustificare un più intenso presenzialismo del giudice sui social media — tratteggiano una identità costituzionale del magistrato diversa da quella di un semplice funzionario statale formato in un lungo, laborioso percorso di studi — le «viginti annorum lucubrationes» di Fortescue, richiamate da Blackstone[200]. *Expressis verbis* riconosciuto come tale, il tentativo è quello di "umanizzare" l'autorità giurisdizionale[201], colmando il fossato, per così dire, "antropologico" che separa l'utente della giustizia dal suo principale dispensatore: disvelandone i tratti personali e quotidiani, l'uso del social media da parte del magistrato «humanizes a branch that is called upon to make life-changing decisions that impact people's lives every day»[202]. L'idea, evidentemente, è che la domanda di giustizia del cittadino sia meglio corrisposta da una persona di cui si conoscono storia, interessi e percorso di vita, piuttosto che da un, per

198 Cfr. *ex plurimis* W.A. Greene (Lord), *Law and Progress* (1944), cit. in R. Stevens, *The English Judges. Their Role in the Changing Constitution*, Oxford, 2005, 26 («*The function of the legislature is to make the law, the function of the administration is to administer the law and the function of the judiciary is to interpret and enforce the law. The judiciary is not concerned with policy. It is not for the judiciary to decide what is in the public interest. These are the tasks of the legislature, which is put there for the purpose, and it is not right it should shirk its responsibility*»); C. Mortati, *Istituzioni di diritto pubblico*, Padova, 1962, 961 («Un altro motivo [per la preferenza del concetto di "ordine" su quello di "potere" nell'art. 104, comma 1, Cost.] può farsi discendere dall'attribuzione alla parola potere di un significato ristretto, di esplicazione di un'attività volitiva: attività che si ritiene estranea al giudice, essendo questi tenuto solo ad emettere giudizi dichiarativi di una volontà altrui cioè di quella del legislatore»); G. Astuti, (testo), in Aa.Vv., *Custodire i custodi*, Milano, 1975, s.i.p. («Nello Stato di diritto il principio della indipendenza del giudice è inscindibile dal principio della sua soggezione alla legge. Non abbiamo un regime di "diritto libero", e sono universalmente noti i canoni razionali dell'ermeneutica giuridica, e i limiti dell'interpretazione giudiziale della legge, costituzionale o ordinaria. [I]n uno Stato democratico l'attuazione della cosiddetta "politica del diritto" appartiene alla competenza normativa propria ed esclusiva del legislatore, e non può essere usurpata dal singolo magistrato in sede di attuazione della concreta volontà di legge nel giudizio, senza attentare al principio di legalità, e con esso alla imparzialità della giustizia»); A. Barak, *The Role of a Supreme Court in a Democracy*, in *Hastings Law Journal*, 5, 2002, 1205 («*The role of the judiciary is to adjudicate disputes according to law*»).

199 «*The judge's robe symbol even if taken as a mere power symbol probably has value in causing the unsuccessful litigant (and it is to be noted that in a lawsuit at least one litigant will be unsatisfied) to accept the decision. The robe depersonalizes the judge and makes him a symbol for the abstract "law", or "the state". […] It should also be observed that this depersonalization of the judge outlines that aspect which we consider so essential to justice that we symbolically concretize it in the blind goddess with scales: complete impartiality*» (R.A. Kessler, *The Psychological Effects of The Judicial Robe*, in *American Imago*, 1, 1962, spec. 53–54).

200 W. Blackstone, *Commentaries on the Laws of England,* cit.

201 Cfr. S.L.A. Dillard - B.M. McCormack, *The Robed Tweeter. Two Judges' Views on Public Engagement,* cit., 195, 197.

202 Ivi, 197.

così dire, "apatico" tecnico del diritto[203]. In questo processo di umanizzazione cruciale diventa allora la condivisione da parte del giudice degli aspetti più intimi e quotidiani della propria vita[204].

L'insoddisfazione per una visione della magistratura come algido apparato burocratico meramente dedito ad una complessa operazione intellettuale — l'applicazione del diritto a casi concreti — dovrebbe del resto risuonare familiare al giurista italiano. Per l'importanza della sede e l'influsso esercitato, il pensiero corre innanzitutto alla celebre relazione di Maranini a Gardone, ove — puntellata da una problematica concezione giusrealista dell'interpretazione giuridica[205] — si sostenne la tesi della necessaria compartecipazione della magistratura alla funzione di indirizzo politico costituzionale: «[i]l giudice deve sempre ricordarsi che in maggiore o minor misura egli è produttore di diritto, e che tutta la sua *coscienza umana*, e dunque anche il suo *indirizzo politico*, *si proietta inevitabilmente nelle sue decisioni*»[206]. Il rigetto della visione tradizionale ha poi trovato altri eminenti teorizzatori[207], che hanno esplicitato chiaramente la necessità di una

[203] L'accusa di «apatia» ricorre non a caso con frequenza nel pensiero di quanti, rigettando la «traditional view», invocano «profonde trasformazioni organizzative» nell'organizzazione della giustizia, al fine di «ridurre la distanza che separa la straordinaria profondità e creatività della funzione giudiziaria odierna e l'organizzazione a essa preposta, originariamente pensata per un corpo di pubblici dipendenti il cui carattere maggiormente apprezzato era l'apatia sociale e l'abitudine di nascondere le proprie decisioni dietro un burocratico "ita lex"» (G. Zagrebelsky, *Il diritto mite. Legge, diritti, giustizia*, Torino, 1992, 206).

[204] «*In our view, it is crucial for judges' social-media accounts to be accurate reflections of who they are in real life. Authenticity resonates. […]. One way to be authentic is to discuss your interests outside of the law. The people you serve are interested in knowing what kind of person you are when you take off the robe; so share your hobbies and passions with them. We recognize that some of our colleagues may find it unusual or even unseemly for a judge to disclose aspects of his or her personal life to the public, but we think doing so humanizes judges and makes us more accessible to the people we serve. In our view, accessible judges and courts promote greater confidence in the judiciary*» (S.L.A. Dillard - B.M. McCormack, *The Robed Tweeter. Two Judges' Views on Public Engagement,* cit., 195). Per un vivido ritratto delle modalità di una forte presenza "personale" del giudice sui social media v. sempre ivi, 196.

[205] Maranini richiama il giusrealista Cardozo per affermare la necessaria creatività giurisprudenziale anche nelle esperienze di *civil law* a causa dell'indeterminatezza dello *ius scriptum*, per cui «[i]l giudice, quale interprete per la comunità del suo senso del diritto e dell'ordine, deve supplire alle omissioni, correggere le incertezze e armonizzare i risultati della sua attività di interpretazione con la giustizia mediante un metodo di libera decisione» (G. Maranini, *Funzione giurisdizionale ed indirizzo politico nella Costituzione. Relazione al XII Congresso Nazionale Magistrati Italiani*, in Aa.Vv., *Atti e commenti XII. Congresso nazionale, Brescia-Gardone 25-28-IX-1965*, Roma, 1966, 22). Tuttavia, il realismo giuridico non ha mai predicato l'«indeterminatezza radicale» delle fonti del diritto, quanto piuttosto quella «locale», che in nessun modo fa venir meno il postulato — anzi, lo presuppone — che «*the proper institutional role of judges in a democracy is simply to apply the law and to enforce the will of the legislature*», per dirla con il più importante interprete moderno della Scuola americana (B. Leiter, *Legal Indeterminacy*, in *Legal Theory*, 3, 1995, 487; per la differenza tra «radical» e «local indeterminacy», che differenzia il realismo giuridico da prospettive come i *Critical Legal Studies* v. sempre id., *Naturalizing Jurisprudence. Essays on American Legal Realism and Naturalism in Legal Philosophy*, Oxford, 2007, spec. 11–12, 18, 77–78).

[206] G. Maranini, *Funzione giurisdizionale ed indirizzo politico nella Costituzione. Relazione al XII Congresso Nazionale Magistrati Italiani,* cit., 24 (corsivo aggiunto).

[207] Il riferimento, tra gli altri, può essere al celebre «uso alternativo del diritto», su cui il rimando è ovviamente ad alcuni dei saggi collezionati in P. Barcellona (a cura di), *L'uso alternativo del diritto*, II voll., Roma-Bari, 1973, ed in particolare a L. Ferrajoli, *Magistratura democratica e l'esercizio alternativo della funzione giudiziaria*, in cui, muovendo dal rilievo per cui il giudice non può essere «semplice voce della legge» in quanto «in qualsiasi ordinamento, anche il più perfetto e il più rigoroso, il giudice deve sempre operare delle scelte tra le diverse interpretazioni tecniche che sono associabili alla maggior parte delle norme che egli è chiamato ad applicare» (ivi, 107) — scelte che «avvengono necessariamente sulla base di criteri che tecnico-giuridici non sono, e che sono criteri metagiuridici di valore aventi carattere etico o ideologico

nuova «duplice posizione» della magistratura rispetto allo Stato e, disgiuntamente, alla società: «una specialissima e difficilissima posizione, che non ha riscontro in nessun altro caso di pubblici funzionari, di intermediarietà tra lo Stato (in quanto potere politico-legislativo) e la società (in quanto sede dei casi che avanzano pretese in nome dei principî costituzionali), una intermediarietà, per cosí dire, immediata che la distingue dalla posizione dell'amministrazione, mediata dalla gerarchia e dalla responsabilità» e da cui deriverebbe una «doppia dipendenza, nel senso di doppia fedeltà, e una doppia indipendenza, nel senso di relativa autonomia, nei confronti sia dell'organizzazione che esprime la legge, sia della società che è titolare di pretese costituzionalmente garantite»[208]. A loro volta, il superamento della «traditional view» e la conseguente affermazione di un legame diretto con la società civile hanno giocato un ruolo nell'evoluzione dell'"autocoscienza" di parte della magistratura, connotandone nel profondo gli sviluppi[209] e portando ad inevitabili tensioni con il potere politico rappresentativo[210].

o più genericamente politico» (ivi, 107–108) — e che pertanto — coerentemente — non può parlarsi «dell'attività giudiziaria come di un'attività tecnica e neutrale, oggettivamente fedele alla legge» (ivi, 108), bensì di una funzione che «*è*, perché non può non essere, politica» (ivi, 106), l'A. sosteneva la necessità di «una maturazione politica del giudice che può compiersi solo attraverso una radicale trasformazione dei suoi modelli di comportamento e dei suoi abiti mentali» (ivi, 118). Essenziale al rinnovamento delle strutture sociali appariva allora proprio un diverso coinvolgimento del giudice con la società di riferimento: «in tanto sarà possibile un esercizio alternativo della funzione giudiziaria in quanto esso si fondi su di un costume e su di una prassi a loro volta alternativi rispetto ai tradizionali modelli di condotta del giudice borghese: in quanto, cioè, il giudice *si apra all'esterno*, e superando la *chiusura corporativa* e *castale* del proprio ruolo rompa l'isolamento fittizio in cui lo vuole la cultura dominante e *si collochi all'interno delle dinamiche sociali*, mediante un impegno politico vissuto non già, idealisticamente e moralisticamente, come impegno tutto individuale e soggettivo, bensì come partecipazione diretta allo scontro politico in collegamento organico con il movimento di classe» (ivi, 119, corsivi aggiunti). L'«emancipazione politica del giudice» e il «suo collegamento con l'esterno» risultano «condizioni necessarie perché una giurisprudenza alternativa possa svilupparsi e progredire […]: l'identificazione della separazione dal popolo della magistratura come casta e del giudice come singolo quale fattore di spossessamento della sovranità popolare in ordine a una funzione di potere quale è quella giudiziaria. Questo spossessamento e questa separazione non sono che un aspetto del più vasto processo di espropriazione politica del popolo attuato dallo Stato borghese rappresentativo nel quadro della più generale separazione tra istituzioni statali e società civile, tra pubblici poteri e sovranità popolare» (*ibidem*). Più di recente, riferimento di una visione del potere giudiziario alternativa a quella tradizionale può certamente considerarsi il celebre settimo capitolo di G. Zagrebelsky, *Il diritto mite. Legge, diritti, giustizia,* cit., 179 ss.

208 Ivi, 206–207.

209 Cfr. diffusamente S. Senese, *Relazione*, in Aa.Vv., *Atti del Seminario su "La magistratura italiana nel sistema politico e nell'ordinamento costituzionale" (cenni storici e problemi). Pisa, 28 aprile 1977*, Milano, 1978, 44–87.

210 «L'alta conflittualità che dalla metà degli anni 80' ruota attorno alle denunce del corporativismo correntizio e della politicizzazione del CSM affonda le proprie radici nel decennio precedente, allorché si manifestano le prime tensioni tra magistratura e ceto politico legate a inchieste giudiziarie e si sviluppa la prima fase di espansione *de facto* delle competenze» (S. Benvenuti, *Il Consiglio superiore della magistratura francese. Una comparazione con l'esperienza italiana*, Milano, 2011, spec. 12–13). Al riguardo v. R. Canosa - P. Federico, *La magistratura in Italia dal 1945 a oggi*, Bologna, 1974, spec. 303 ss.; E. Scoditti, *Il contropotere giudiziario. Saggio di riforma costituzionale*, Napoli, 1999, spec. 23 ss.; A. Meniconi, *Storia della magistratura italiana*, Bologna, 2012, 321 ss.; E. Bruti Liberati, *Magistratura e società nell'Italia repubblicana*, Bari-Roma, 2018, spec. 109 ss. A sua volta, la conflittualità istituzionale ha reso problematica qualsiasi iniziativa di riforma organica dell'ordinamento giudiziario, dietro cui può stagliarsi il sospetto di una «rivincita» del potere politico rappresentativo sul potere giudiziario: «la perpetuazione di un clima di rivincita della classe politica verso la magistratura rende più difficili riforme, come quella dell'ordinamento giudiziario, che aspettano oltre cinquant'anni e sono costituzionalmente necessarie» (G. Silvestri, *Lo stato senza principe. La sovranità dei valori nelle democrazie pluraliste*, Torino, 2005, 143). Per converso, al crescere della

Come già peraltro notato dalla dottrina[211], il problema della regolamentazione dell'uso dei social media da parte dei magistrati sembra allora far riaffiorare risalenti alterità di vedute sul ruolo del giudice nella società, sulla sua "identità costituzionale" e correlativamente sulla «"funzione sociale" della giurisdizione»[212]. Giustificare la preferibilità di una delle due impostazioni è sforzo che va, evidentemente, al di là degli spazi di questa indagine e delle capacità di chi scrive — e, per certi versi, oltre le colonne d'ercole della stessa scienza giuridica. Certo non si fa mistero qui della maggiore affinità con la più tradizionale impostazione, almeno nel momento in cui si sente di appartenere alla schiera di quanti sono disposti a pagare il prezzo di una magistratura «isolated or out of touch»[213] se questo è il costo di un più alto livello di imparzialità e indipendenza del magistrato[214]. Senza contare poi che un utilizzo "libertario" dei social media da parte del magistrato dovrà essere valutato non solo alla stregua del corretto assolvimento della funzione giurisdizionale, per come definita anzitutto nel Titolo IV della Carta costituzionale, ma anche secondo il metro dei requisiti di «disciplina ed onore» cui tutti i depositari di «funzioni pubbliche» devono conformarsi ex art. 54, c. 2, Cost.[215].

conflittualità con la politica è seguito un certo appianamento delle divisioni in seno alla magistratura associata: v. M. Volpi, *Le correnti della magistratura. Origini, ragioni ideali, degenerazioni*, in *Rivista AIC*, 2, 2020, 365–366. Per la comprensione della dialettica tra politica e magistratura fondamentali restano gli apporti della scienza politica (*ex plurimis* v. A. Pizzorno, *Il potere dei giudici. Stato democratico e controllo della virtù*, Roma-Bari, 1998, spec. 67–99) e della sociologia giuridica (cfr. E. Moriondo, *L'ideologia della magistratura italiana*, Bari, 1967, spec. 313–342).

211 A questa discussione — o se non altro alla sua "prima fase" — fa riferimento S. Sica, Social *media e magistratura*, *cit*, 546, quando richiama il «significativo dibattito — oggi, apparentemente meno d'attualità — sul ruolo "sociale" e, dunque, "politico" della magistratura […] particolarmente sentito alla fine degli anni '60, allorché si arrivò addirittura ad ipotizzare un ruolo "militante" della magistratura».

212 «[T]esi inaccettabile se accostata ad un'idea "eversiva" o "alternativa" del diritto, ma pienamente coerente ed auspicabile con un obiettivo "promozionale" della produzione giurisprudenziale» (ivi, 564).

213 ABA, Formal Opinion 462, cit.

214 I primi commenti della dottrina italiana paiono innanzitutto concordi sull'inquadramento della vicenda nei termini della "contrapposizione tradizionale" tra libertà del magistrato *uti civis* e tutela dell'imparzialità della funzione giurisdizionale: cfr. P. Sammarco, *Giustizia e social media,* cit., 143; L. Longhi, *I magistrati e l'uso dei* social. *Appunti sulla deontologia professionale di categoria nell'era della comunicazione di massa,* cit., 195; S. Sica, *Social media e magistratura*, cit., 565; A. Lollo, *Libertà di manifestazione del pensiero e uso dei social da parte dei magistrati,* cit., *passim*. A favore di un approccio "restrittivo", nel senso descritto del testo, mi sembra si possano poi leggere le pregnanti considerazioni di S. Sica, *Social media e magistratura*, cit., 565, che criticando l'idea dell'«esclusione di illecito disciplinare da uso dei mezzi della comunicazione, nel timore di porre in discussione, in prima battuta, la libertà di manifestazione del pensiero del singolo giudice, in seconda, autonomia ed indipendenza dell'istituzione» richiama l'attenzione sul «disegno costituzionale» che regge il potere giudiziario, anch'esso informato «al modello dei pesi e contrappesi»: «non può esservi l'attribuzione di un potere (e di un giustificabile regime di attenuazione di responsabilità), né si possono invocare autonomia ed indipendenza, se non si accetta il *self restraint* sul piano delle prerogative individuali. E lì dove non arriva la sensibilità individuale, è indispensabile che intervenga l'organo di autogoverno oggi piú di ieri baluardo contro una deriva nell'uso della Rete» (*ibidem*). Del resto, rileva sempre efficacemente Sica, «[u]n simile cómpito è il miglior tributo ad una magistratura autonoma ed indipendente, tale perché credibile; con il valore aggiunto di svolgere, per questa via, un cómpito autenticamente sociale, oltre il perimetro della sola categoria. Se c'è da attendersi una giurisprudenza sempre piú capace di fare argine rispetto al tempo dei "leoni da tastiera", gli *haters*, a maggior ragione un simile auspicio è da coltivare nella giurisprudenza di autogoverno» (*ibidem*).

215 Sulla clausola si v. innanzitutto in generale G. Lombardi, voce *Fedeltà (dir. cost.),* cit., 173–175; Id., *Contributo allo studio dei doveri costituzionali*, Milano, 1967, 175 ss.; L. Ventura, *La fedeltà alla Repubblica*, Milano, 1984, 123 ss.; Id., *Art. 54*, in G. Branca - A. Pizzorusso (a cura di), *Commentario della Costituzione*,

Ciò che in ogni caso si voleva enfatizzare, e si spera di aver dimostrato, è semplicemente la significatività del nesso concettuale tra la particolare questione di politica del diritto — *idest,* a quali condizioni permettere, o addirittura richiedere, l'utilizzo dei social media da parte dei magistrati — e la più generale concezione del ruolo del potere giudiziario nella democrazia costituzionale, che a sua volta si riallaccia a problemi di teoria generale del diritto e dell'interpretazione giuridica[216]. L'esortazione dunque, per l'interprete come per il *policymaker*, è ad una trattazione della specifica questione *de iure condendo* in una prospettiva di ampio respiro, anche — se non soprattutto — al fine di evitare il consolidamento di punti di caduta discrasici nella legislazione: se infatti è valore condiviso la coerenza ordinamentale, appare del tutto inopportuno permettere — o addirittura a richiedere — un ampio e disinibito utilizzo dei social media da parte di soggetti che si vogliono, al contempo, il più possibile terzi ed imparziali; viceversa, si appalesa un controsenso bollare come «a wise but entirely detached body of individuals» un ordine professionale cui si è fortemente compresso l'accesso ad uno dei più significativi luoghi della socialità contemporanea[217].

4. Conclusione

Per quanto possa senz'altro affermarsi che le esigenze di imparzialità e indipendenza della magistratura si applichino al contesto dei social media con la stessa forza con cui insistono sui tradizionali mezzi di comunicazione, trattare i primi alla stregua dei secondi rischia di rappresentare una sottovalutazione della, per così dire, "ontologia" dei mezzi digitali, le cui particolarissime modalità sembrano invece insidiare in modo affatto nuovo l'identità costituzionale del magistrato: come ben sintetizza proprio il giudice americano, infatti, «*the use of social media websites […] presents concerns unique to the role of the judiciary in our justice system*»[218]. Al di là del condivisibile invito ad una formazione dedicata del giudice[219] — fino alla teorizzazione di un vero e proprio «duty of

Bologna-Roma, 1993, part. 82 ss.; G.M. Salerno, *Art. 54*, in R. Bifulco - A. Celotto - M. Olivetti (a cura di), *Commentario alla Costituzione*, Torino, 2006, 1081 ss.; A. Morelli, *Articolo 54*, in F. Clementi - L. Cuocolo - F. Rosa - G. E. Vigevani (a cura di), *La Costituzione italiana. Commento articolo per articolo*, II ed., vol. I, Bologna, 2021, spec. 362–363. Sull'applicazione della disposizione ai magistrati v. N. Battello, *Considerazioni sulla responsabilità penale dei magistrati*, in Aa.Vv., *Giudicare il Giudice. Sugli aspetti costituzionali, civili, penali e amministrativi della responsabilità del magistrato*, Milano, 1982, 198; M. Pivetti, *Il Csm scopre il Berufsverbot*, e A. Pignatelli, *Sul dovere di fedeltà*, entrambi in *Quest. giust.*, 4, 1982, 889 ss., 909 ss.; P. Petta, *Una sentenza poco "fedele" alla Costituzione*, in *Crit. dir.*, 1983, 169 ss.; A. Cerri, *Sul principio di fedeltà (a proposito di una recente decisione della Sezione disciplinare del C.S.M.)*, in *Riv. trim. dir. pubb.*, 3, 1983, 761–762; M.C. Folliero, *La legge n. 194 del 1978 nella giurisprudenza della Corte costituzionale. Dal monito al controllo di come il monito sia attuato*, in *Giur. cost.*, 1988, spec. 1363 ss.; A. Pignatelli, *Problemi di responsabilità disciplinare*, in *Quest. giust.*, 2–3, 1994, 246–247; C. Salazar, *La magistratura*, Roma-Bari, 2002, spec. 143–144.

[216] Il riferimento è al già ricordato richiamo al realismo giuridico nordamericano da parte di Maranini nella sua celebre relazione a Gardone, così come alle riflessioni di Ferrajoli e Zagrebelsky.

[217] Sulla possibilità di equiparare i social media a «*public forum*» cfr. per tutti M. Bassini, *Libertà di espressione e social network, tra nuovi «spazi pubblici» e «poteri privati». Spunti di comparazione*, in questa *Rivista*, 2, 2021, 75 ss.

[218] *Youkers v. State*, 400 S.W.3d 200, 205 (Tex. App.–Dallas 2013).

[219] «*Although, like everyone else, judges can take part in social media, like everywhere else, judges must anticipate*

tech competence»[220] — le difficoltà incontrate nella gestione del fenomeno da parte di un sistema giudiziario pure informato a standard di comportamento magistratuale non tassativamente tipizzati — e pertanto teoricamente più resistenti ai mutamenti tecnologici — dovrebbero considerarsi un monito sull'unicità del "registro letterario" dei social media, che non solo pare irriducibile ai tradizionali mezzi di comunicazione e socialità, ma in qualche modo non sembra nemmeno assoggettabile ad una gestione unitaria, come vividamente dimostra l'"estremo regolatorio" di raccomandazioni disciplinari personalizzate in funzione delle diverse piattaforme digitali.

Benché si siano menzionati i motivi che potrebbero rendere attrattivo un approccio restrittivo all'utilizzo dei social media da parte dei magistrati, non si è qui articolata una vera e propria proposta *de iure condendo* sull'ottimale punto di caduta tra i contrapposti interessi in gioco. Piuttosto, alla luce dell'esperienza statunitense — insostituibile pietra di paragone per le altre legislazioni comparate — si è sviluppata una più circostanziata riflessione in riferimento alla valutazione comparativa degli interessi in gioco: in particolare, si è sostenuto che la risoluzione della questione di politica del diritto dipenda da due diverse ricostruzioni degli interessi costituzionali rilevanti, che a loro volta accedono ad alternative concezioni del ruolo della magistratura nello Stato costituzionale di diritto.

Ad emergere nitidamente, in ogni caso, in una conclusiva visione d'insieme, sono i tratti ossimorici che assume il problema della regolamentazione dell'utilizzo dei social media da parte dei magistrati[221]. Da una parte, la specifica questione di politica del dirit-

intensive scrutiny on social media and accept burdensome restrictions that do not apply to other users. Thus, a judge should not try her hand at social media unless she is committed to doing the initial work and making the continuing effort necessary to comply with the code of judicial conduct while friending, tweeting, Instagramming, or otherwise posting» (C. Gray, *Stumbling Online*, cit., 26). Nello stesso senso v. *CGUE Opinion 25/2022*, 18: «*Understanding which social media platforms are in use, how the various social media platforms operate, what type of information it may be appropriate to share on various social media platforms and which potential risks and consequences participation in such platform communication might have, would be an appropriate area for training judges. The training should cover technical aspects (such as the different privacy settings of different social platforms), aspects of profiling and data protection. The judiciary should provide training to newly appointed judges and to permanent judges on a continuous basis. Associations of judges may contribute to training, exchanging and sharing knowledge and best practices among judges*». Pregnante anche l'impegno espresso dall'organo di autogoverno della magistratura amministrativa italiana: «I magistrati amministrativi hanno il diritto ed il dovere di ricevere una formazione specifica relativa ai vantaggi e ai rischi derivanti dall'utilizzo dei social media; al riguardo, vanno previste, a cura del Consiglio di Presidenza della Giustizia Amministrativa e dell'Ufficio studi della Giustizia amministrativa, nelle forme più idonee ed efficaci, iniziative di aggiornamento e formazione in materia» (*Delibera CGA*, cit., 3). Nella dottrina italiana v. E. Bruti Liberati, Un punto di arrivo, cit., 320–321, e implicitamente S. Sica, Social media e magistratura, cit., 537, laddove afferma che «[s]arebbe interessante, a titolo esemplificativo, verificare tra la platea di utenti "specialisti" e qualificati per definizione, come i magistrati, quanti hanno chiaro che, a dispetto della "gratuità" apparente del servizio, essi stanno sottoscrivendo un contratto; contratto, di natura atipica, "gratuito", nel senso della prestazione a carico di una sola parte (il gestore del *network*)».

[220] J.G. Browning, *Should Judges Have a Duty of Tech Competence?*, cit., 179.

[221] Di una dimensione paradossale nella regolamentazione dell'utilizzo dei social media da parte dei magistrati parla anche, sebbene in un senso diverso, Mitchell: «*For the judiciary, social media presents a paradox. On the one hand, the independence and integrity of the judiciary depends upon the public's perception — a perception increasingly shaped by new media. Social media provide an invaluable tool for public outreach, allowing courts and judicial candidates to inform the public about the role of the courts, recent judicial decisions, or even judicial campaigns. On the other hand, a judge's use of that media can jeopardize the public's perception of a verdict, decision, or even the judiciary itself. The rare instance of egregious misconduct could quickly embed in the popular consciousness*» (N.J. Mitchell, *Judge*

to presenta dinamiche inedite, capaci di mettere a dura prova il tradizionale armamentario concettuale della giustizia disciplinare: non solo, dunque, le categorie dell'irrigidita tipizzazione disciplinare italiana, ma anche quelle classiche formule ad ampio respiro che continuano a connotare la responsabilità del giudice negli ordinamenti comparati. Da altra parte, il problema riporta all'attenzione alcuni nodi irrisolti del diritto pubblico generale — la collocazione costituzionale della magistratura ed il suo ruolo nella società — con radici che puntano nel profondo delle più alte questioni di teoria generale del diritto e dell'interpretazione giuridica. Proprio in questo intreccio tra un fenomeno di assoluta novità — i social media — e una risalente questione di teoria costituzionale — la collocazione della magistratura nelle Stato costituzionale di diritto — deve al tempo stesso vedersi il fascino del problema *de iure condendo*, che invita il giurista — e perché no, a livello diverso, il legislatore stesso — al "salutare strabismo" di chi deve guardare tanto *indietro* — ai fondamenti delle moderne democrazie costituzionali e al mai sopito dibattito sul ruolo del potere giudiziario — quanto *avanti* — alle novità e alle irriducibilità della società tecnologica contemporanea[222].

2.0. A New Approach to Judicial Ethics in the Age of Social Media, cit., 2157–2158).

[222] «*[A] judge's conduct on the Internet and social media raises questions old and new that go to the heart of fair trials and impartial justice*» (H.B. Dixon Jr., *Judicial Ethics and the Internet (Revisited)*, in *Judges' Journal*, 4, 2018, 39).

The regulatory road to the European Media Freedom Act: opportunities and challenges ahead*

Vincenzo Iaia

Abstract

This paper presents an overview of the evolution of the European media regulation and recent developments. The analysis is made up of three main parts: (i) an analysis of the European legal framework in the media field before the EMFA; (ii) a comparison with foreign media regulations – especially those enacted in Florida and Texas – and case-law; (iii) an assessment of the challenges and opportunities that are likely to arise from the EMFA in the current ever-growing "phygital" world.

Summary

1. The European background

The digital platform-based economy has *inter alia* reshaped how content is created, distributed and consumed. Consequently, the media landscape has shifted dramatically over the last twenty years. For instance, millions of European families now watch online content on mobile devices rather than sitting in front of the TV[1]. It would not be hasty to acknowledge that social media platforms have transformed into the new public town square[2]. If on the one hand such a scenario has made access to information more democratized, on the other hand the information provided does not necessarily originate from regulated sources, as it can come from amateur and unreliable ones or, even worst, from entities interested in manipulating the electoral processes

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco"

[1] European Commission, Press release *Revision of the Audiovisual Media Services Directive (AVMSD)*, 23 September 2021, available at the following link: Digital-strategy.ec.europa.eu/en/policies/revision-avmsd.

[2] Florida Senate Bill no. 7072, 24 May 2021, Sec. 1, para. 4.

and/or polarising the public opinion[3].

A recent example of the social media platforms' power in the dissemination of information and misinformation can be seen with the Coronavirus Disease 2019 pandemic (and infodemic), complicating the corresponding public health response[4].

Established literature describes media and press as the "fourth estate" or the "fourth power" because of its watchdog function over the well-functioning of the other free powers[5]. Historically, newspapers were regarded as guardians of the interests of the people[6]. The blooming of new actors delivering information has created new dynamics and regulatory gap at the expenses of traditional elite media organizations. The ever-growing laws in this field are aimed to iron out some of these inconsistencies by enhancing media pluralism and freedom in the increasingly digitised and globalized world. Indeed, such values are regarded as *sine qua non* preconditions for the rule of law, and, as a result, essential safeguards for a healthy democracy[7].

It should be premised that the European intervention in the media sector was originally confined to the regulation of electronic commerce and audiovisual services. The e-Commerce Directive[8], adopted in 2000, limited liability for intermediary service providers, allowing public discourse over the Internet to flourish without any major boundaries. In particular, Arts 12, 13 and 14 of the E-Commerce Directive set out the so-called safe harbor system by allowing certain online intermediaries, including hosting providers, to be exempted from liability for the hosting of unlawful content[9] uploaded by users of their service, unless they fail to comply with the notice and take down mechanism. Moreover, art. 15 expressly exonerated digital platforms from a general obligation to monitor the activities carried out by their users.

As such, the E-Commerce Directive created the legal conditions for the rise and development of the Internet infrastructure and the information society. In fact, at the start of the millennium, about 20 years ago, the Internet was almost an unexplored

[3] Y.M. Citino, *Verso l'European Media Freedom Act: la strategia europea contro le minacce al pluralismo e all'indipendenza dei media da una prospettiva de iure condendo*, in *Rivista di Diritto dei Media*, II, 2022, 2.

[4] J.A. Gallo - C.Y. Cho, *Social Media: Misinformation and Content Moderation Issues for Congress*, Congressional Research Service, 2021, 1.

[5] J. Rowbottom, *Media Law*, Oxford, 2018, 2, 3, highlighting that media is powerful because a set of media institutions has the capacity to expose abuses of power and inform the audience on a scale not found with most other speakers. See also G.A. Borchard, *The SAGE Encyclopedia of Journalism*, II ed., Thousand Oaks, 2022, 675, and the here-cited bibliography.

[6] W.T. Stead, *Government by Journalism*, in *The Contemporary Review*, 49, 1886, 653.

[7] R. Mastroianni, *Freedom of pluralism of the media: an European value waiting to be discovered?*, in *Rivista di Diritto dei Media*, I, 2022, spec. 100, 101 e 103, relying upon three decisions of the European Court of Human Rights (ECHR) underscoring the inextricable link between freedom of expression and pluralism, namely ECHR, *Informationsverein Lentia and Others v. Austria*, app. 13914/88 (1993); ECHR, *Centro Europa 7 S.R.L. v. Italy*, app. 38344/09 (2012); ECHR, *Associazione Politica Nazionale Lista Marco Pannella et Radicali Italiani v. Italy*, app. 20002/13 (2021).

[8] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular, electronic commerce, in the Internal Market, L 178.

[9] The notion of unlawful content can cover several types of activities (from intellectual property infringements to defamation, hate speech, and terrorism-related speech) depending on each national law.

and risky land. No company would have the financial and technical resources to monitor the massive amount of information daily uploaded by their users. From a socio-economic perspective, the safe harbor was the most efficient policy option to direct investments towards what will become a strategic sector worldwide.

The first European intervention in the audiovisual sector dates to 1989 with the enactment of the Televisions Without Frontiers Directive (TVWF Directive)[10]. The Directive rests on two basic principles: (i) the free movement of European television programmes within the internal market and (ii) the requirement for TV channels to reserve, whenever possible, more than half of their transmission time for European works ("broadcasting quotas"). The TVWF Directive also safeguards certain important public interest objectives, such as cultural diversity, the protection of minors and the right of reply.

In December 2005, the Commission submitted a proposal to revise the TVWF Directive to broaden its scope considering the growing popularity of non-linear television services. After five years, the EU adopted the Audiovisual Media Service Directive[11] ("AVMSD"). The AVMSD Directive covered more than just traditional linear television and shared similar objectives of the previous regulation, being aimed at breaking down the barriers that hinder the proper functioning of a single European market for audiovisual media services, while contributing to the promotion of cultural diversity, and providing an adequate level of protection for consumers and minors. This regulatory framework has facilitated the emergence of a vibrant market, as witnessed by the following data:

almost 9.000 TV channels were established in the EU at end 2013 and about 2.000 of them had a cross-border dimension;

there were over 2.500 VOD services in the EU at end of 2014, 195 of them being established in one Member State and targeting another Member State;

between 2009 and 2013, EU broadcasters' net revenues grew by 2.9% (from 69.6 billion to 71.6 billion euros) whereas VOD online revenues (including taxes) grew from 248 million in 2009 to 1,526 million (up 515%)[12].

For a few years, it appears that the AVSMD reached its objective of enhancing the prosper of a dynamic market of audiovisual services across Europe[13]. However, the fast-evolving changes arising from the digital technologies led the European Commission ("EC") to propose a revision of the AVMSD[14] ("revised AVMSD"), which was

[10] Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by Law, Regulation or Administrative Action in Member States concerning the pursuit of television broadcasting activities, OJ L 298

[11] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services, L 95/1.

[12] Commission Staff Working Document, *A Digital Single Market Strategy for Europe – Analysis and Evidence*, 6 May 2015, SWD (2015) 100 final, para. 4.2.

[13] R. Viola, *La riforma del quadro normativo dell'audiovisivo tra mercato unico digitale e valori fondamentali*, in E. Apa - G. Abbamonte - O. Pollicino (eds.), *La riforma del mercato audiovisivo europeo*, Torino, 2019, XII.

[14] Directive 2018/1808/EU of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media

approved by the European Parliament and the Council in 2018. The revised AVMSD offers many new elements, such as:

- an extension of certain audiovisual rules to video sharing platforms and social media services[15];
- better protection of minors against harmful content in the online world, including strengthening protection on video-on-demand services[16];
- reinforced protection of TV and video-on-demand against incitement to violence or hatred, and public provocation to commit terrorist offences[17];
- favour for product placement[18];
- increased obligations to promote European works for on-demand services[19];
- more flexibility in television advertising, allowing broadcasters to choose more freely when to show ads throughout the day[20];
- independence of audiovisual regulators[21] and official establishment of the European Regulators Group for Audiovisual Media Services[22] (ERGA)[23].

It is worth noting that art. 1(a) of the TWFD directive defined "television broadcasting" as the «transmission of programmes intended for the general public» while art. 1(a) of the AVMSD Directive adopted the same definition to define an audiovisual media service but adds that service providers carried editorial responsibility when they exercise an effective control both over the selection of the programmes and over their organisation.

A comprehensive look at the European legal framework outlines a tension between this last provision and the liability exemption provided by the E-Commerce Directive. To this purpose, Recital 25 of the Revised AVSMD tries to find a consistent solution

services (Audiovisual Media Services Directive) in view of changing market realities, L 303/69.

15 Art. 1, revised AVMSD.

16 Art. 6a, revised AVMSD.

17 Art. 6, revised AVMSD.

18 Art. 11, revised AVMSD. Recital 93 of the AVSMD looked unfavorably on product placement by stating that «sponsorship and product placement should be prohibited where they influence the content of programs in such a way as to affect the responsibility and the editorial independence of the media service provider».

19 Art. 13, para. 1 of the revised AVMSD obliges Member States to ensure that on-demand audiovisual media service provides secure at least 30% share of European works in their catalogs and ensure prominence of those works. Art. 13, para. 2 of the Directive also allows Member States to require media service providers to contribute financially to the production of European works, including via direct investment in content and contribution to national funds.

20 According to art. 23, para. 1 of the revised AVMSD, the overall limit is set at 20% of broadcasting time between 6:00 to 18:00 with the same share allowed during prime time (from 18:00 to midnight). Recital 87 of the AVSMD required companies to organize advertisements hourly, having maximum 12 minutes per hour. The *ratio* under the increased flexibility in the management of advertisements resides on greater consumer choice since the advent of online media platforms.

21 In compliance with art. 30 of the revised AVMSD, the regulatory authorities designated by Member States should be legally distinct from the government and functionally independent of their respective governments and of any other public or private body.

22 Art. 30b, revised AVMSD. The group has existed since 2014, being a forum for the exchange of best practices amongst national authorities.

23 European Commission, Press release *Revision of the Audiovisual Media Services Directive (AVMSD)*, cit.

with the two (opposite) regimes by limiting editorial responsibility to those services the principal purpose of which is the provision of programmes in order to inform, entertain or educate.

However, with so much audiovisual content now online, the boundary between services that fall under the AVMSD and those eligible for the safe harbour under the E-Commerce Directive (ECD) had become increasingly blurry[24]. Expanding (or restricting) the scope of the AVMSD entails a delicate balancing exercise amongst freedom of expression and freedom to conduct a business, with major consequences for national media industries and for consumers. This thorny issue has also been addressed by the proposal for the European Media Freedom Act (see *infra* para. 3).

In recent years, a more horizontal and direct approach to media issues has replaced the sector-specific intervention. Europe's response counts various soft law acts, including the EP resolution on media pluralism and media freedom in the European Union[25], the recommendation of the Council of Europe on media pluralism and transparency of media ownership[26], the EC Communication on the European democracy action plan[27], the EC Communication on Europe's Media in the Digital Decade[28], the EC recommendation on ensuring the protection, safety and empowerment of journalists and other media professionals in the European Union[29]. As regards hard law acts, the European Commission has issued a proposal for a directive on protecting persons who engage in public participation from manifestly unfounded or abusive court proceedings[30].

In addition to direct measures, European institutions have indirectly addressed media issues through collateral regulations. One of the most prominent packages of measures is to tackle the knotty problem of platform liability for illegal activities carried out by third parties on digital platforms[31]. To that end, art. 17 of the Copyright in

[24] S.B. Micova, *The Audiovisual Media Services Directive*, in P.L. Parcu - E. Brogi (eds.), *Research Handbook on EU Media Law and Policy*, Cheltenham, 2021, 264.

[25] European Parliament Resolution of 3 May 2018 on media pluralism and media freedom in the European Union (2017/2209(INI)).

[26] Recommendation of the Committee of Ministers to Member States on media pluralism and transparency of media ownership, 7 March 2018, CM/Rec (2018)1[1].

[27] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European democracy action plan, 3 December 2020, COM (2020) 790 final.

[28] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Europe's Media in the Digital Decade: An Action Plan to Support Recovery and Transformation, 3 December 2020, COM (2020) 784 final.

[29] Recommendation of the Commission on ensuring the protection, safety and empowerment of journalists and other media professionals in the European Union, 16 September 2021, COM (2021) 6650 final.

[30] European Commission, Proposal for a directive of the European Parliament and the Council on protecting persons who engage in public participation from manifestly unfounded or abusive court proceedings ("Strategic lawsuits against public participation"), 27 April 2022, COM (2022) 177 final.

[31] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Online Platforms and the Digital Single Market. Opportunities and Challenges for Europe, 25 May 2016, COM (2016) 288

the Digital Single Market Directive[32] (CDSM Directive) focuses on platform liability for copyright infringements for the content uploaded by their users. This provision should be read in tandem with art. 2 (g), of the proposal for a Single Market For Digital Services[33] (Digital Services Act or DSA) which adopts a broader approach to the notion of unlawful content by covering any information which, in itself or by its reference to an activity, including the sale of products or provision of services, is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law. The DSA pursues the wider goal of formalizing private ordering measures into legislatively mandated obligations, under a stricter application of the principle of proportionality and protection of fundamental rights, thus promoting constitutionalisation of platform responsibility[34].
The catalogue of initiatives indirectly touching media issues is further enriched with Creative Europe, the project within the Next Generation EU[35] with a budget of € 2.53 billion to develop innovative audiovisual content, provide support to the news media sector, foster pluralism and cross-border collaboration, and promote media literacy. Lastly, the Regulation on contestable and fair markets in the digital sector[36] (Digital Markets Act or DMA), aimed at ensuring dynamic competition in markets where gatekeepers are present, can guarantee a certain degree of media diversity as well as respect for consumer autonomy and choice[37].

2. Transatlantic food for thought: selected case-law in the U.S.

The regulation of the media industry is similarly at the epicentre of a vigorous debate in the U.S. Since 1996, Section 230 of the Communications Decency Act[38] has allowed

final; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms, 28 September 2017, COM (2017) 555 final.

[32] Directive 2019/790/EU of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market, L 130/92.

[33] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act), 15 December 2020, COM (2020) 825 final.

[34] G. Frosio, P*latform Responsibility in the Digital Services Act: Constitutionalising, Regulating and Governing Private Ordering*, in A. Savin - J. Trzaskowski (eds.), *Research Handbook on EU Internet Law*, forthcoming, 2022.

[35] Next Generation EU is a € 800 billion temporary instrument designed to boost recovery from the Covid-19 pandemic. For more information see European Union, Next Generation EU, available at the following link: next-generation-eu.europa.eu/index_en.

[36] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), L 265/1.

[37] For some comments on the DMA, see M. Wörsdörfer, *The Digital Markets Act and E.U. Competition Policy: A Critical Ordoliberal Evaluation*, in *Philosophy of Management*, forthcoming 2022; A. De Streel (ed.), *The European proposal for a Digital Markets Act. A first assessment*, Centre on Regulation in Europe, Brussels, 2021.

[38] 47 U.S. Code, Section 230, Protection for private blocking and screening of offensive material, 1996.

almost absolute freedom of online speech, shaping the Internet as we got to know it[39]. According to the provision, «No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider».

This broad immunity does not cover the content that infringes criminal law, electronic communications privacy law, and intellectual property law [40]. It implies that conducts sanctioned as torts rather than crimes are considered less harmful than intellectual property infringements. For instance, in *Jones v Dirty World Entertainment Recordings*[41], the owner and operator of the popular gossip site www.thedirty.com escaped liability despite encouraging defamatory statements[42]. If the plaintiff had filed a complaint grounded on copyright infringement for the sharing of a picture, for example, the hosting provider would have risked liability if it failed to remove it[43].

The interpretation of Section 230 represents a hostile battleground between the Democrats and the Republicans. While the formers have increasingly been challenging Section 230, asking for more regulatory tools to fight disinformation and illegal and harmful speech, the latter have frequently criticised deplatforming and content moderation as censure mechanisms.

In 2021, Florida[44] and Texas[45], both ruled by Republican governors, passed two acts imposing content moderation restrictions and disclosure requirements on social media platforms. These laws have been challenged as violating the First Amendment on the grounds that they hinder the platforms' ability to speak through content moderation. Indeed, platforms are prohibited to deprioritise certain types of content resulting in hate speech or disinformation. The Conservatives complain that social media platforms discriminate against them by suspending or shadow-banning their account for sharing political speech. In contrast, platforms counterargue they only enforce rules against hate speech or misinformation.

---

[39] J. Kosseff, *The twenty-six words that created the Internet*, New York, 2019.

[40] As regards liability for copyright infringement(s) in the digital environment, the Digital Millennium Copyright Act ('DMCA') can be considered as equivalent to the E-commerce directive. Indeed, Section 512 of the DMCA introduced a notice and take down regime excluding an Internet service provider from being liable on the condition that it «(A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material; (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; (C) upon notification of claimed infringement as described in paragraph, responds expeditiously to remove, or disable access to, the material that is claimed to be infringing to be the subject of infringing activity». For a worldwide perspective of the intermediary liability regulation and Internet users' rights, see the World Intermediary Liability Map provided by the Stanford Center for Internet and Society at the following link: *wilmap.law.stanford.edu*.

[41] U.S. District Court, 6th circuit, decision of 6 June 2014, no. 13-5964.

[42] E.B. Laidlaw, *What is a joke? Mapping the path of a speech complaint on social networks*, in D. Mangan - L.E. Gillies (eds.), *The Legal Challenges of Social Media*, Cheltenham, 2017, 140.

[43] *Ibidem*.

[44] Florida Senate Bill no. 7072, 24 May 2021.

[45] Texas House Bill no. 20, 9 September 2021.

The U.S. Courts of Appeals have recently taken opposite positions on whether these laws are likely to violate online platform constitutional free speech rights[46]. On the one hand, the Eleventh Circuit[47] largely upheld a preliminary injunction ruling on the Florida Senate Bill as likely to be unconstitutional, preventing the law from taking effect. On the other hand, the Fifth Circuit[48] rejected this challenge regarding the similar Texas law. The two decisions have been referred to the U.S. Supreme Court to settle the case law contrast.

Additionally, the U.S. Supreme Court was tasked with resolving two other significant cases related to the social media landscape.

In *Twitter Inc. v. Taamneh*, the Supreme Court decided whether Twitter was jointly liable for aiding and abetting an act of terrorism under Section 2333 of the Antiterrorism Act[49]. The plaintiff accused Twitter of having hosted pro-ISIS content that communicated the terrorist group's message, radicalized new recruits, and furthered its mission. The Ninth Circuit declined to consider Section 230 in this case. Moreover, it held that Twitter, Google, and Facebook could be liable for aiding and abetting an act of international terrorism because they provided generic, widely available services to billions of users, some of whom were allegedly supporters of ISIS[50]. The Supreme Court[51] rejected this theory highlighting the lack of concrete causal nexus between the creation (and the provision) of social media platforms and the ISIS attack. Indeed, bad actors can use cell phones, email, or the Internet but the producers of these services/infrastructures cannot be deemed liable simply for having granted access to them. According to the Judge Clarence Thomas the «companies relationship with ISIS and its supporters appears to have been the same as their relationship with their billion-plus other users: arm's length, passive, and largely indifferent». The Supreme Court affirmed that the plaintiffs' allegations did not show that Twitter knew and gave substantial assistance to ISIS in the Reina attack. There was also any evidence that Twitter gave ISIS any special assistance for the success of this attack. However, Justice Ketanji Brown Jackson specified in a brief concurring opinion that the safe harbour have no unlimited boundaries by stressing that «other cases presenting different allegations and different records may lead to different conclusion».

In *Reynaldo Gonzalez v. Google LLC*, the Court was called upon to determine whether tech platform recommendation algorithms were shielded from lawsuits under Section 230 of the Communications Decency Act. The case involved claims against Google (as a mother company of YouTube) for direct and secondary liability due to its algorithms recommending ISIS-created content. The Ninth Circuit concluded that most of the plaintiffs' claims were barred by Section 230 since the algorithms did not treat

[46] V.C. Brannon, *Free Speech Challenges to Florida and Texas Social Media Laws*, Congressional Research Service, 22 September 2022, available at *crsreports.congress.gov*.

[47] U.S. Court of Appeal, 11th circuit, decision of 23 May 2022, no. 21-12355.

[48] U.S. Court of Appeal, 5th circuit, decision of 16 September 2022, no. 21-511.

[49] Antiterrorism and Effective Death Penalty Act of 1996, Public Law no. 104-132.

[50] U.S. Court of Appeal, 9th circuit, decision of 22 June 2021, no. 18-17192.

[51] U.S. Supreme Court, decision of 18 May 2023, no. 21-1496, *Twitter Inc. v. Taamneh et al.*

ISIS-created content differently from other third-party content[52]. The Supreme Court endorsed this reasoning stating that much (if not all) of plaintiffs' complaint fail under the *Twitter Inc. v. Taamneh* decision[53]. As regards to the other charges, there was no proof that Google reached an agreement with ISIS or that it intended to intimidate or coerce a civilian population, or to influence or affect the government.

The common interpretative problem stemming from the two mentioned cases concerns the breadth of the editorial control that can be expected of online platforms. Indeed, their editorial influence is manifested in the organization of the content rather than its production, as older types of media, such as broadcasting[54]. It seems that time has come to revise the understanding of editorial competence, almost as regards large online platforms. For instance, platforms may be excluded from exercising editorial power when their algorithms display content according to neutral criteria, like the chronological or the alphabetical ones as well as according to users' preferences and interactions[55]. Conversely, algorithms that organize content in ways to polarize users towards a political party witness an editorial influence of the platform. From a technical viewpoint, this presupposes the power to access and examine (and understand!) the computer program in order to understand its effective functioning.

A last glimpse of the fundamental role played by the U.S. Supreme Court in shaping the interpretation of the First Amendment to accommodate the challenges of the digital platform economy emerges in *Mahanoy Area School District v. B.L.*[56]. In the case at hand, the parents of B.L., a cheerleader at Mahanoy Area High School ('MAHS') claimed the violation of the First Amendment because the school suspended their daughter for the upcoming year after being informed that she had posted a picture of herself on Snapchat with the caption «F*** school, f*** softball, f*** cheer, f*** everything». The photo, posted in the weekend and lasting for 24 hours, reached about 250 people, many of whom where student at MAHS and some of whom were cheerleaders.

The Third Circuit upheld a district court injunction[57], ordering MAHS to reinstate B.L. to the cheerleading team because the school lacked authority to regulate this kind of off-campus speech, neither it could invoke the *locus parentis* doctrine[58]. The Supreme Court came to the same conclusion on the grounds that the content has been

[52] U.S. Court of Appeal, 9th circuit, decision of 22 June 2021, no. 18-16700.

[53] U.S. Supreme Court, *Reynaldo Gonzalez v. Google,* no. 21-1333, 2023.

[54] L. Kukliš, *Video-sharing platforms in AVMSD: a new kind of content regulation*, in L. Parcu - E. Brogi (eds.), *Research Handbook on EU Media Law and Policy*, cit., 307.

[55] See also J. Rowbottom, *Media Law*, cit., 351, 352, who argues that another option to avoid editorial liability could be that of arranging the algorithm to ensure that people are confronted with diverse opinions and sources. He interestingly submits that the organization of content according to user's preference might lead that user to get trapped in a "bubble", hearing messages that reflect existing interests rather than diverse views.

[56] U.S. Supreme Court, no. 594 (2021).

[57] U.S. District Court, 3rd Circuit, decision of 21 March 2019, no. 3:17-CV-01734.

[58] The in loco parentis has long been condemned as a principle used to rationalize oppression and even violence against public school students. For a further analysis of the doctrine see *Mahanoy Area School District v. B. L.*, in *Harvard Law Review*, 135, I, 2021, 353 ss.

posted outside of school hours from a location outside the school and did not identify the school or target any member of the school community with vulgar or abusive language. It has also been specified that the school's power to punish off-campus student speech is limited to specific circumstances, like serious bullying or harassment; threats aimed at teachers or other students; failure to follow rules concerning lessons and homework, the use of computers, or participation in online school activities; breaches of school security devices. Based on these premises, the Supreme Court considered B.L.'s post as not involving features that would place it outside the First Amendment's ordinary protection[59].

3. The European Media Freedom Act: main features and possible challenges ahead

On 10 January 2022, the European Commission launched a public consultation to collect views by relevant interested parties on the most important issues affecting the functioning of the internal media market. According to Věra Jourová, Vice-President for Values and Transparency, «Media are a pillar of democracy. But today this pillar is cracking, with attempts by governments and private groups to put pressure on the media. This is why the Commission will propose common rules and safeguards to protect the independence and the pluralism of the media. Journalists should be able to do their work, inform citizens and hold power to account without fear or favour […]»[60].
The consultation focuses on three core areas of media markets: (i) how to guarantee transparency and independence of media providers (e.g., scrutiny of media market transactions, transparency of media ownership[61] and audience measurement); (ii) which conditions trigger their healthy functioning (e.g., exposure of the public to a plurality of view, media innovation in the EU market, freedom of journalism); (iii) how to ensure fair allocation of state resources (e.g., independence of public service media, transparency and fair distribution of state advertising).
The call attracted 917 responses, most of which supported the idea of a legislative proposal based on a principle-based approach rather than detailed standard-setting or no action at all. However, each type of stakeholder expressed its own needs and concerns. In particular, non-governmental organisations and public service broadcasters

[59] Justice Stephen Breyer, the Judge who wrote the opinion for this case, expressed its concerns of crystallizing in the decision the specific circumstances under which the school would have a special interest in regulating off-campus speech: «Particularly given the advent of computer-based learning, we hesitate to determine precisely which of many school-related off-campus activities belong on such a list. Neither do we now know how such a list might vary, depending upon a student's age, the nature of the school's off-campus activity, or the impact upon the school itself». For further thoughts see M. Coyle, *Justice Breyer scouts a path through a sticky thicket of student speech*, National Constitution Center, 25 June 2021, available at *constitutioncenter.org*.

[60] European Commission, press release *European Media Freedom Act: Commission launches public consultation*, 10 January 2022, available at *ec.europa.eu*.

[61] On the heterogeneous legal framework concerning media ownership see R. Crafurd Smith - B. Klimkiewics - A. Ostling, *Media ownership transparency in Europe: Closing the gap between European aspiration and domestic reality*, in *European Journal of Communication*, 36, 2021, 547 ss.

were in favour of an EU-level action to introduce safeguards for editorial independence, seeking guidance on the appropriate prominence of audiovisual media services of general interests. Private broadcasters supported the introduction of common principles for media pluralism measures and audience measurement, like transparency, objectivity, and verifiability. Conversely, publishers expressed a general preference for self-regulation. Citizens voice the need for transparency and fairness in the allocation of state advertising. Finally, broadcasters and publishers share the urge to set out an effective regulation for online platforms.

On 16 September 2022, the European Commission tries to bring together all the opinions in the proposal for a regulation establishing a common framework for media services in the internal market[62] (European Media Freedom Act or EMFA). The proposal is aimed at achieving balanced and impartial media coverage, based on transparency, deeper regulatory convergence and cooperation between Member States, and an enabling environment for innovative media. The pressure for specific treatment of media companies arises from their crucial role in effectively ensuring democracy across European Member States by providing access to a plurality of views and reliable sources of information to citizens and businesses alike.

The proposal takes account of the ongoing disruption of the media industry in the fast-changing digital environment which has also blurred the line between independent and corporate-owned media providers[63]. The need to preserve media companies' independence and transparency has gained momentum in order to fight against the erosion of fundamental rights, namely freedom of expression and information, as well as media freedom and pluralism. Indeed, these rights, explicitly protected by art. 11 of the European Charter of Fundamental Rights[64], are currently under threat due to the fragmented responses across European Member States[65]. Hence, the EMFA is founded on the premise that transparency and independence of media undertakings must be ensured through a horizontal instrument based on maximum harmonisation. Such consideration is bolstered by the fact that the media sector falls within the 14 key ecosystems for an inclusive and sustainable recovery and for the European economy's twin (green and blue) transition[66].

Getting into *medias res*, the EMFA covers several key aspects for the preservation and promotion of media industries, dealing with (i) safeguards for the independent and transparent functioning of public service media providers; (ii) strengthening the pow-

[62] Proposal for Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market, 16 December 2022, COM (2022)457 final.

[63] World Economic Forum, White Paper *Understanding Value in Media: Perspectives from Consumers and Industry*, Geneve, 2020, 12.

[64] Charter of Fundamental Rights of European Union, 26 October 2012, C 326/391. See also the Protocol no. 29 on the system of public broadcasting in the Member States, annexed to the Treaties, 26 October 2012, C 326/1, affirming that «the system of public broadcasting in the Member States is directly related to the democratic, social and cultural needs of each society and on the need to preserve media pluralism».

[65] See in particular the study commissioned by the European Parliament *The fight against disinformation and the right to freedom of expression*, July 2021, available at *europarl.europa.eu*.

[66] EMFA, 1.

er of the European Board for Media Services; (iii) stricter rules for providers of very large online platforms; (iv) the introduction of a right of customisation of audiovisual media offer; (v) the assessment of media market concentrations.

Art. 5 deals with independence of public service organizations (PSOs), requiring them to provide in an impartial manner a plurality of information and opinions. They should also appoint their management through a transparent, open, and non-discriminatory procedure. Moreover, Member States should ensure that PSOs have adequate and stable financial resources for the fulfilment of their public service mission. The ambitious goal is to grant independence of editorial board from the property of the media entity. This is very delicate because every Member State has its own attitude on this. For instance, in Italy, whereas there is a clear regulation dealing with the independence of the journalists *vis à vis* the directors and owners, there are no rules about independence of editors *vis à vis* ownership because it is considered protected under the freedom to conduct a business[67]. The relationship between editors and owners falls within the freedom to conduct a business. It is just governed by labor law, according to which the owner can fire the editor without justification because of the fiduciary duty of this job.

Art. 6 contains the guarantees of transparency with which media service providers should comply. They can be divided into disclosure and organizational obligations. As regards the former, media service providers should disclose (a) their legal name and contact details; (b) the names of their direct or indirect owners with shareholdings enabling them to exercise influence on the operation and strategic decision making; (c) the names of their beneficial owners. For what it concerns the latter, media service providers should take measures that (a) guarantee editors' freedom over their editorial decisions; (b) ensure disclosure of any actual or potential conflict of interests.

Arts. 8-12 set up the European Board for Media Services. The new Board should replace the ERGA and receive further tasks and responsibilities, having a pivotal role in the implementation of the new legal framework. Amongst the several tasks provided by art. 12, the Board shall draw up opinion with respect to enforcement measures in case of disagreement between two national authorities on the actions for the effective enforcement of the obligation to ensure the right of reply in the case that a natural or legal person has been damaged by an assertion of incorrect facts in a television programme, pursuant to art. 28 AVSMD[68]. It should also assist the Commission in establishing common guidelines with respect to factors to be taken into account when applying the criteria for assessing the impact of media market concentrations[69]. Despite its proclaimed independence, there are different cases that condition Board's action upon the agreement of the Commission. There is an ongoing negotiation as to how increase the distance between the Commission and the Board[70].

Art. 17 establishes a framework of duties intended exclusively for providers of very

[67] O. Pollicino, *PromethEUs workshop on the European Media Freedom Act (EMFA)*, Athens, 20 October 2022.

[68] EMFA, art. 12, lett. e), (ii).

[69] EMFA, art. 12, lett. h), (ii).

[70] M. Killeen, *EU Council's agreement in sight on media freedom*, 8 June 2023, available at *euractiv.com*.

large online platforms[71], including the obligation: (a) to communicate to the media service provider the statement of reasons accompanying the decision to suspend the provision of its online intermediation services in relation to a specific content; (b) to take all the necessary technical and organization measures to ensure that complaints under art. 11 of Regulation 2019/1150/EU[72] are processed and decided upon with priority and without undue delay; (c) to engage in a meaningful and effective dialogue with media service providers that frequently undergo the suspension or restriction of the online intermediation services by the very large online platform without sufficient grounds; (d) to declare that it is subject to regulatory requirements for the exercise of editorial responsibility in one or more Member States, or adheres to a co-regulatory or self-regulatory mechanism governing editorial standards, widely recognised and accepted in the relevant media sector in one or more Member States; (e) to disclose the number of instances where they imposed any restriction or suspension of their services and the grounds for imposing such restrictions.

The stricter accountability framework targeting large professional intermediaries is likewise grounded on an emergent emphasis on corporate social responsibility (CSR)[73]. According to this business model under expansion, undertakings are expected to integrate the current environmental, social, and ethical values into their strategies. Thus, they should consider the impact of their business operations also on freedom of expression and other fundamental rights. These fair and responsible conducts find justification under the Directive on non-financial reporting[74] which requires public-interest companies in EU Member states with more than 500 employees to disclose certain types of non-financial and diversity information in their yearly management reports. On 21 June 2022, the Council and European Parliament reached a provisional political agreement on the corporate sustainability reporting directive (CSRD) to address shortcomings in the existing directive, especially as regards the quality of information delivered to investors[75].

---

[71] The definition of "very large online platforms" is laid down in art. 25 of the Digital Services Act, referred to as «online platforms which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million».

[72] Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, L 186/57.

[73] G. Frosio, P*latform Responsibility in the Digital Services Act: Constitutionalising, Regulating and Governing Private Ordering*, cit., 6. For a multidisciplinary analysis of corporate social responsibility see D. Caterino - I. Ingravallo (eds.), *L'impresa sostenibile. Alla prova del dialogo dei saperi*, EuriConv, Lecce, 2020. See also A. Rasche - M. Morsing - J. Moon (eds.), *Corporate Social Responsibility. Strategy, Communication, Governance*, Cambridge, 2017.

[74] Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups, L 330/1.

[75] The directive will introduce more detailed reporting requirements and ensure that large companies are required to report on sustainability issues such as environmental rights, social rights, human rights, and governance factors. The CSRD will also introduce a certification requirement for sustainability reporting as well as improved accessibility of information, by requiring its publication in a dedicated section of company management reports. For more information see the press release by the Council of the EU, *New rules on corporate sustainability reporting: provisional political agreement between the Council and the European Parliament*, 30 June 2022, available at *consilium.europa.eu*.

At international level, social accountability is rooted in the United Nations (UN) Human Rights Council declaration of Internet freedom as a human right[76], in the UN Guiding Principles on Business and Human Rights[77], and in the preamble of the UN Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises[78].

Art. 19 entitles users of media services to the right of customisation of audiovisual media offer. According to it, manufacturers and developers shall ensure a functionality enabling users to freely and easily change the default settings controlling or managing access to and use of the audiovisual media services offered.

Art. 21 concerns the assessment of media market concentrations. It gives to media authorities a greater say over mergers having an impact on media pluralism and editorial independence. In parallel with the standard antitrust test on whether the merger would entail a substantial impediment to effective competition[79], media market concentrations require further elements to be taken into account, namely: (a) the impact of the concentration on media pluralism, including its effects on the formation of public opinion and on the diversity of media players on the market, taking into account the online environment and the parties' interests, links or activities in other media or non-media businesses; (b) the safeguards for editorial independence, including the impact of the concentration on the functioning of the editorial teams and the existence of measures by media service providers taken with a view to guaranteeing the independence of individual editorial decisions; (c) whether, in the absence of the concentration, the acquiring and acquired entity would remain economically sustainable, and whether there are any possible alternatives to ensure its economic sustainability.

The obligation to consider the impact on the media market arising from the concentration acknowledges the pitfalls of the current antitrust test to ensure democracy as it is exclusively dedicated to guarantee market efficiency[80]. Although for the sake of brevity we cannot dig into antitrust underpinnings, it suffices to note that the approach set out by the EMFA embraces the neo-Brandeis movement (also called hipster antitrust) according to which excessive concentrations does not only yield economic consequences, being able to jeopardize democratic values, too[81]. In this perspective, antitrust authorities should be empowered to block a merger also when it could undermine media freedom. However, the present disagreement on the most

[76] United Nations, resolution of 13 July 2021 on the promotion, protection and enjoyment of human rights on the Internet, A/HRC/47/L.22.

[77] United Nations, Guiding Principles on Business and Human Rights, 16 June 2011, Geneva and New York.

[78] United Nations, Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with regard to Human Rights, 26 August 2003, Geneva.

[79] For an in-depth analysis of the SIEC test see I. Kokkoris - H. Shelanski, *EU Merger Control: An Economic and Legal Analysis*, Oxford, 2014.

[80] On this topic, see widely B.P. Paal, *Current issues and recent developments on media concentration in the context of competition law and media law*, in *Journal of Intellectual Property Law & Practice*, 12, VII, 2017, 610 ss.; K. Bania, *The role of media pluralism in the enforcement of EU competition law*, doctoral thesis discussed at the European University Institute, Florence, 2015.

[81] A thorough explanation and promotion of the New Brandeis school is given by T. Wu, *The Curse of Bigness: Antitrust in the New Gilded Age*, New York, 2018.

reliable indicators to monitor media freedom and pluralism requires ERGA to provide some coordinates in order to apply common standards across the EU[82].

That said, the proposal is not immune from criticism in the light of some controversial issues that it is likely to arise. First and foremost, we refer to the competence conundrum. In this regard, art. 167(5) of the Treaty on the Functioning of the European Union (TFEU) prevents EU from adopting instruments that would harmonize national media laws and regulations, being its competence limited to provide incentive measures and recommendations[83]. The European Commission, aware of this limit, identified the legal basis of the EMFA in art. 114 TFEU, which is basically the wildcard provision to extent European competences over the borders established by the Treaties. Indeed, it empowers the EU to approximate the provisions adopted by Member States which have as their object the establishment and functioning of the internal market.

The CJEU has adopted a restrictive interpretation of art. 114 TFEU in *Commission v Council*[84], under which it has been affirmed that «Recourse to Article 114 TFEU is not justified where the measure has only the incidental effect of harmonizing market conditions within the Union»[85]. It is true that media might come under the category of internal market interventions, which is shared competence, but it also might be regarded as falling within culture, where only supporting action is allowed[86]. The creation of categories of competence inevitably creates difficulties in deciding which aspects of social policy fall within the boundaries and which overcome them.

The EMFA seems to deal with some aspects that are supposed to be regulated by national laws as having only incidental effects to the market. Indeed, the state interference in public service media, the restrictions to sources and communications of journalists as service providers, the strategies to enhance media pluralism seem to fall within the constitutional identity of the Member States and their political sovereignty. From this point of view, the EMFA stretches legal competence of the EU through a regulation – the most invasive policy instrument – in a field whereby the EU legislative power appears to be limited to soft law acts[87]. It should be reminded that back in

[82] E. Brogi - R. Carlini - I. Nenadić - P. Luigi Parcu - M. Viola de Azevedo Cunha, *EU and media policy: conceptualising media pluralism in the era of online platforms. The experience of the Media Pluralism Monitor*, in P.L. Parcu - E. Brogi (eds.), *Research Handbook on EU Media Law and Policy*, cit., 16 ss.

[83] M.D. Cole - J. Ukrow - C. Etteldorf, *On the allocation of competences between the European Union and its Member States in the media sector. An analysis with particular consideration of measures concerning media pluralism*, Institute of European Media Law, 2020, available at *orbilu.uni.lu*; A. Garcia Pires, *Media Pluralism and Competition*, in *European Journal of Law and Economics*, vol. 43, II, 2017, 255-283.

[84] CJEU, decision of 18 November 1999, Case C-209/97, *Commission v. Council*, EU:C:1999:559.

[85] *Ivi*, para 35.

[86] P. Craig - G. de Búrca, *EU Law: Text, Cases, and Materials*, 7th ed., Oxford University Press, Oxford, 2020, 115, passim.

[87] In even stronger terms see V. Zeno-Zencovich, *The EU regulation of speech. A critical view*, in *Rivista di Diritto dei Media*, I, 2023, 16, 17, who clearly outlines that «The summit of Commission's invasion of the field of freedom of expression is represented by […] the "European Media Freedom Act. […] The intention of regulating "media service providers" is simply a way of extending – completely *ultra vires* – the competences of the Commission […]». For an opposite perspective see G. Muto, *European Media Freedom Act: la tutela europea della libertà dei media*, ivi, III, 2022, 225.

1995, the European Commissioner Mario Monti tried to harmonize media pluralism in a proposal of directive which has been rejected by Germany and United Kingdom because of the lack of competence by the EU over media issues[88]. The above-mentioned arguments persuaded some scholars to argue that, as EU law currently stands, a recommendation seems to be the most suitable instrument to incorporate media policies[89]. Nonetheless, a minority position has submitted that the differences in Members States' legislations in media independence, restrictions on media ownership by person holding public office, and contrast to dominant positions in the mass media markets are evident threats to the functioning of the internal market, leading undertakings to find some Member States more appealing than others to establish or invest[90]. Taking these diverging opinions into account, it would not be surprising if Member States will challenge the validity of art. 114 TFEU as legal basis of the EMFA before the CJEU.

Moreover, it has been clear for Europe that online platforms play a key role in the content organization, but they do not bear editorial responsibility over the content to which they provide access. The EMFA tackles this issue by considering providers of video-sharing platforms and very large online platforms as media service providers for the sections of their services in which they exercise an editorial power[91]. To this purpose, a media service provider is defined as a natural or legal person whose professional activity is to provide a media service and who has editorial responsibility for the choice of the content of the media service and determines the way it is organised[92]. Hence, the classification as media service provider prevents any escape from liability exemption(s) and create a legitimate expectation to act diligently as well as to provide information that is trustworthy and respectful of fundamental rights.

As much as the new legal framework can be welcome, it raises some practical questions. They especially relate to the determination of the threshold of influence above which an online platform can also be considered as media service provider. It is not clear how to identify the specific sections subjected to the editorial power of the provider. This requires a disclosure obligation on how the content are organized. But what if the content organization and moderation is delegated to algorithms, especially those equipped with Artificial Intelligence (AI)[93]? One solution could be that of con-

88 For wider comments see S. Kaitatzi-Whitlock, *Pluralism and Media Concentration in Europe: Media Policy as Industrial Policy*, in *European Journal of Communication*, 11, IV, 1996, 453 ss.

89 M.D. Cole - J. Ukrow - C. Etteldorf, *On the allocation of competences between the European Union and its Member States in the media sector. An analysis with particular consideration of measures concerning media pluralism*, cit.; A. Garcia Pires, *Media Pluralism and Competition*, cit.

90 R. Mastroianni, *Freedom of pluralism of the media: an European value waiting to be discovered?*, cit., 106.

91 EMFA, Recital 8.

92 EMFA, art. 2, para. 1.

93 As noted by G. Frosio, P*latform Responsibility in the Digital Services Act: Constitutionalising, Regulating and Governing Private Ordering*, cit., 3, 4, «The terms of the debate that online content moderation entails, via filtering and monitoring and the use of automated tools in particular, has been spelled out by the Court of Justice of the European Union (CJEU) multiple times. When imposing obligations on internet service providers a trifecta of interests must be taken into consideration, including the freedom of those service providers to conduct a business, guaranteed in Article 16 of the Charter, the fair balance between that freedom, the right to freedom of expression and information of the users of

sidering the (natural or legal) person deploying such a computer program accountable for its choices, thus piercing the algorithmic veil.

A more reasonable policy option could be to pretend that the service provider would disclose its algorithm to the media authority in order to allow an expert to assess the extent to which the computer program can influence the organization of content. Although for some people AI appears as a black box[94], there is an increase of studies devoted to Explainable AI, which is a research area aimed at allowing humans to understand the processes and methods followed by machine learning algorithms to reach a certain result or to produce a specific content[95]. As such, the need of an explainability-by-design approach to AI systems cannot be ignored no more in view of granting a fair allocation of responsibilities. This is bolstered by the fact that platforms may be incentivised to set the algorithm to take down all the contents that slightly – if not remotely – infringe other parties' rights to quickly avoid any risk of liability. Such an excessive prudent approach would likewise hinder freedom of expression since it risks turning into private censorship.

Another issue pertains to the enforcement of the EMFA. In the early reaction by Civil Liberties Union for Europe to the proposal, it has been argued that the EMFA fails to offer strong oversight on how existing and newly established media rules will be enforced[96]. The Commission has for years declined to launch investigations against the Member States, such as Hungary or Poland (the main targets of some intrusive interventions), where free media is under threat. The EMFA tries to deal with such democratic asymmetries in the Eastern Europe[97] through a regulation. But the problem is that, as being a regulation, this law is supposed to apply all over Europe, where the issue of editorial independence is less striking. Hence, the regulation should contain more detailed enforcement measures for those Member States where systemic attacks to democracy are perpetrated. A proportionate response to media issues across the EU requires a granular approach based on the level of media freedom ensured in each Member State, considering that some stronger measures would not be necessary for those States where the media market operates well.

Finally, some press publishers argue that the EMFA will have the opposite effect than

their services, enshrined in Article 11 of the Charter, and the right to intellectual property of the rightholders, protected in Article 17(2) of the Charter». Compare CJEU C-314/12, *UPC Telekabel Wien GmbH vs. Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH* (2014); CJEU, C-401/19, *Republic of Poland v European Parliament and Council of the European Union* (2022), § 80.

[94] On this topic see A. De Streel - A. Bibal - B. Frenay - M. Lognoul, *Explaining the black box: when law controls AI*, Centre on Regulation in Europe, Brussels, 2020; F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge, 2016.

[95] R. Hamon - H. Junklewitz, I. Sanchez, *Robustness and Explainability of Artificial Intelligence. From technical to policy solutions*, Publications Office of the European Union, Luxembourg, 2020; A. Adadi - M. Berrada, *Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)*, in *IEEE Access*, 6, 2018, 52138-52160.

[96] Liberties, *Liberties' Comment on the European Commission's European Media Freedom Act Proposal*, 16 September 2022, available at *liberties.eu*.

[97] The 2022 Rule of law report of the European Commission of 13 July 2022, COM(2022) 500 final, invites Poland, Rumania, Slovenia, Slovak, Check Republic, Hungary and Cyprus to strengthen the rules and mechanisms to enhance the independent governance of public service media taking into account European standards on public service media.

that of protecting media organizations from political and economic meddling[98]. New publishers' lobbies fear the regulation could affect their editorial power over their publications, advocating for a proportionate approach in support of Member States' power to guarantee media pluralism and freedom of expression[99]. According to this perspective, there is no need to adapt systems of public service media governance that are already performing good in ensuring their independence.

4. Concluding remarks

The proper functioning of media companies is quintessential for ensuring freedom of expression and information, which are in turn a relevant litmus paper to measure the effective level of democracy. The urge to preserve media companies' independence and transparency has gained momentum in the digital platform economy whereby content are produced, distributed and consumed according to innovative channels. The disruption of the media industry with the progressive emergence of important new players has also blurred the line between independent and corporate-owned media providers. This may constitute a threat to art. 11 of the EU Charter of Fundamental Rights, aimed at granting freedom of expression and information, as well as media freedom and pluralism.

National interventions to curb media freedom and pluralism backsliding in Member States seem to be inadequate, considering the cross-border nature of digital platforms. A homogeneous legal response can originate at European level inasmuch it complies with the subsidiarity[100] and proportionality[101] principles. In this regard, the European Union has issued several acts of soft and hard law to govern the digital platform economy so as to unleash its unique opportunities. Some of them directly address media issues while others are more generally intended to make Europe fit for the digital age. The puzzle of legal policies in the media field is complicated by their uncertain target, considering that some online operators (social media, search engines and application platforms) fall into the grey zone of providing user-generated content with an undetermined control over their ranking and moderation[102]. This is exacerbated by the different standards applied by Member States to measure the audience of media organizations even if it is crucial to ascertain their real market positioning[103]. However,

98 C. Goujard. *We're fine as we are, Press tells EU as Brussels plans media freedom law*, in *Politico.eu*, 16 September 2022, available at *politico.eu*.

99 Nordvision, *Response to European Commission public consultation for a European Media Freedom Act*, 6 March 2022, available at *nordvision.org*.

100 Art. 5, para. 3, TEU.

101 Art. 5, para. 4, TEU.

102 According to A. Koltay, *New Media and Freedom of Expression. Rethinking the Constitutional Foundations of the Public Sphere*, Bloomsbury, London, 2019, 83, all these online operators «routinely make 'editorial' decisions on making content unavailable, deleting or removing it (whether to comply with a legal obligation, to respect certain sensibilities, to protect their business interests or to act at their own discretion)».

103 Y. Citino, *Verso l'European Media Freedom Act: la strategia europea contro le minacce al pluralismo e*

it appears undisputed that large media undertakings cannot longer rely on private (dis) ordering, made up of diverse forms of self-regulation, like ethics code, press and media councils, or ombudspersons[104]. These operators are often not neutral in relation to the content they display – especially search engine results or feed on social networks – since they discriminate between messages by prioritizing or shadow-banning them according to biased criteria, regardless of their origin from humans or algorithms (which are in any case designed by humans)[105].

The EMFA represents an ambitious milestone to protect the rule of law for the preservation and promotion of quality media services by strengthening the free and pluralistic media system across Europe. Apart from requiring substantial coordination with the existing EU *acquis*, which constitutes a patchwork of direct and indirect measures, there is a heated debate over the most suitable policy tool to address media issues, together with its enforcement and potential unintended consequences. The new regime will not apply to all online actors, but only to those covering a special position to influence their users' ability to access information and their interaction with it, thus fulfilling a democratic function by acting as facilitators of users' speech, creativity and exchange of ideas[106]. To this purpose, scholars have pointed out that information gatekeepers should bear the delicate responsibility to support the public interest, assuming an obligation as trustees of the greater good based on the social function of information[107].

The media regulation is in great ferment also in the U.S., representing a further animated battleground between Republicans and Democratics. The U.S. Supreme Court is playing a central role for the development of media law, assessing whether and to which extent the current rules can accommodate the multiple challenges arising from the increasingly pervasive use of digital platforms. In *Mahanoy Area School District v. B. L.*, the Supreme Court sided for freedom of expression. It would be interesting to analyse how the two contrasts between District Courts concerning the interpretation

all'indipendenza dei media da una prospettiva de iure condendo, cit., 13; V.H. Tien Vu, *The online audience as gatekeeper: The influence of reader metrics on news editorial selection*, in *Journalism*, 2014, 1094-1110.

[104] Indeed, allowing digital platforms to self-regulate the traffic of content risks that effectiveness of the protection against unlawful moderation will depend on the willingness of the platform to remove the content according to its own standards. See for instance Facebook community standards: «Governments also sometimes ask us to remove content that violates local laws but does not violate our Community Standards. If after careful legal review, we find that the content is illegal under local law, then we may make it unavailable only in the relevant country or territory». See also the speech by President of the European Commission von der Leyen at the European Parliament Plenary on the inauguration of the new President of the United States and the current political situation, Brussels, 20 January 2021, according to which «No matter how right it may have been for Twitter to switch off Donald Trump's account five minutes after midnight, such serious interference with freedom of expression should be based on laws and not on company rules. It should be based on decisions of parliaments and politicians and not of Silicon Valley managers».

[105] J. Rowbottom, *Media Law*, cit., 351.

[106] N. Elkin-Koren - M. Perel, *Guarding the Guardians: Content Moderation by Online Intermediaries and the Rule of Law*, in G. Frosio (ed.), *The Oxford Handbook of Online Intermediary Liability*, Oxford, 2020, 669-678.

[107] A. Shapiro, *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*, II ed., New York, 2000, 225.

of Section 230 of the Communications Decency Act will be handled. Considering the growing role of EU as a standard setter, we can infer – or almost hope – that the U.S. Supreme Court will align the next landmark rulings to the higher standards that are likely to set out by the EMFA (unless it will be reviewed by the CJEU).

In conclusion, the complex marvels of cyberspatial communication may create difficult legal issues[108] and many official institutions in the world, legislators or Courts based on the respective legal system, are seeking to keep up with them by balancing the different fundamental rights in tension for the healthy functioning of the fourth power in a democratic society.

[108] The adage was quoted by the U.S. District Court for the Southern District of New York, decision of 4 May 2000, *UMG Recordings Inc. vs. Mp3.com Inc.*, no. LEXIS 5761.

Ethics by design and international soft and hard standards on the nexus gender-artificial intelligence*

Cristiana Carletti

Abstract

The contribution is intended to debate over the nexus between gender and artificial intelligence as for programs and systems based on AI which could produce, if the ethics by design is not approached according to a gender perspective, gender biases. The need for overcoming this criticality rests upon the need for improving the presence and participation of the female component in the design, development and implementation of the aforementioned programs and systems, in digital teams as members or leaders, to contribute for the elaboration of technical solutions within a legal framework which is aimed to translate current soft standards in force into hard laws.

Summary

Keywords

gender - artificial intelligence - ethics by design - soft law - hard standards

1. Setting the scene and the need for a gendered ethics by design towards hard laws

The speediness in the automated processing and use of digital technologies, with particular reference to artificial intelligence, is a social reality. Public and private actors, in charge for the advancement of studies, research and analysis on methodologies of data collection, storage and management, have embraced this challenge since early

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

years of this century and, in pandemic times, have confirmed this approach for the identification of organizational solutions for restructuring and making operational their respective systems through a series of basic algorithms in artificial intelligence programs[1]. Regardless of the meaning attributed to algorithms used in such programs[2], it is clear that their functionality rests on the quantitative and qualitative nature of data under analysis as input data, for producing result as output data[3]. It is the first component of digital data, its volume, that has a decisive impact on the creation of biases, due to subjective choices when selecting, collecting and analyzing data, which is not isolate but rather continuous along the setting of algorithms that allow artificial intelligence programs to operate[4].

Indeed, next to the definition of data categories analyzed by algorithms as for their generality, accuracy, reliability in an objective way, it is the setting of this operation by the designer that could contribute to the occurrence of technical or intentionally dependent biases in the subjective analysis and interpretation of data. This depends upon the setting of algorithms' inquiry to produce categorical output data, which is limiting as to information in terms of quantity - as opposed to the analysis on overall data - as well as quality. At the same time the subjective factor affects the technological design, implying a potential duplication of the analysis of the phenomenon in a biased and discriminatory perspective.

The nexus between the potential development of digital knowledge and its use in such a way as to result in a discriminatory impact in a broad sense, if not also in the gender dimension, has not yet promoted a careful legal analysis such as to anticipate the dynamics inherent in the management of rights and freedoms compressed in an individual capacity as well as the activation of the competencies of judicial and para-judicial bodies for the purpose of remedy in favor of the injured parties.

Some attempts at normative production have been characterized by a soft relevance, distinguishing the commitment to the protection of standards referable to the protection of fundamental rights in charge of public and private actors, although always in a collaborative perspective.

These preliminary exercises are leading, with some effort, to the compilation of secondary legislation in the European Union system and complex legal instruments with binding impact in the framework of the Council of Europe, focused on the best ways to regulate technological apparatuses, particularly those generated and managed through artificial intelligence.

In the first case, the proposed Regulation on Artificial Intelligence (so-called Artificial Intelligence Act) proposed by the European Commission in April 2021, on which the European Parliament approved its negotiating position on June 14, 2023, appears particularly important[5].

---

[1] L. Downey, *Algorithms*, Investopedia, 2021.

[2] J. Guszcza, *Smarter together: Why artificial intelligence needs human-centered design*, Deloitte, 2018.

[3] J. Denny, *What is an algorithm? How computers know what to do with data*, The Conversation, 2020.

[4] A. Manasi - S. Panchanadeswaran - E. Sours - S.J. Lee, *Mirroring the bias: gender and artificial intelligence*, in *Gender, Technology and Development*, 26, 2022, 295 ss.

[5] EU Commission, Communication from the Commission to the European Parliament, the Council, the

The human-centric interpretation offered by the EU institutions rests on the *acquis* of rights and freedoms set forth in the Charter of Fundamental Rights, subject to severe limitations depending upon the use of artificial intelligence in 'high-risk' situations: respect for human dignity, private and family life, protection of personal data, freedom of expression and information, assembly and association, the principle of non-discrimination, and several set of individual and collective rights also relevant in the social and economic domains as well as the judicial system, including in these cross-references gender equality.

It is precisely the gender component (encompassing gender identity and sexual orientation, race, ethnic origin, migratory status, political or religious orientation, or otherwise other discriminatory factors) to be expressly mentioned since the degree of risk and intrusiveness of artificial intelligence-based systems determines profiling by reason of highly sensitive elements that are altered with extreme ease: for example biometric data, personal choices related to the educational and training system up and professional opportunities preferred and pursued by women and girls.

Following these considerations, the European Parliament asserted that «diversity, non-discrimination and fairness' means that AI systems shall be developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases that are prohibited by Union or national law».

On the other hand, the Council of Europe system has set its reasoning in a similar and parallel way, resting on the need for a human rights-based approach in the process of compiling a binding legal instrument dedicated to artificial intelligence and algorithmic technologies[6].

In order to ensure a reinforcing shift for human rights' protection from soft to hard law, the Committee tasked with analysing legal prerequisites underpinning such an instrument recommended the need to include «a provision on respect of equal treatment and non-discrimination of individuals in relation to the development, design, and application of AI systems to avoid unjustified bias being built into AI systems and the use of AI systems leading to discriminatory effects».

The translation of this recommendation into a high-impact binding provision could be set up firstly by introducing an obligation on public and private actors to ensure that artificial intelligence and algorithmic systems are designed to promote the principle of non-discrimination, thus also gender equality; additionally, the obligation requires a wider substantial perspective to include the attribution of a definite mandate to equality bodies, ombudspersons, and independent national human rights institutions

European Economic and Social Committee and the Committee of the Regions, Fostering a European approach to Artificial Intelligence; EU Commission, Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts; as for the EP position, Draft Compromise Amendments on the Draft Report, Doc. KMB/DA/AS, 16 May 2023, Decision by Parliament, 1st reading, 14 June 2023.

[6] As examined further on in the contribution, see Council of Europe-CAHAI Feasibility Study on a legal framework on AI design, development and application based on Council of Europe standard (2020) and Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law (2021) – see note 23.

in monitoring and identifying the impact of algorithms in a discriminatory logic; the adoption of a proportionality test that technically and punctually assesses algorithmic metrics from a discriminatory perspective; the introduction of a general obligation of transparency to value the fairness of technical solutions adopted by digital professionals in the definition of artificial intelligence-based mechanisms; and finally the formulation of an indirect obligation – otherwise positive obligations - for the purpose of adopting preventive assessing tools over algorithmic discriminatory biases in the framework of policies aimed at achieving *de jure* and *de facto* equality.

Such operational proposals, when transposed into a legally binding instrument, could be the best legal prerequisite for incentivizing not only public authorities but also private actors to collaborate for the elaboration and adoption of 'equality by design' technical models.

In this latter perspective, gender biases emerge when, in identifying artificial intelligence programs running, possibly similar to human reasoning, the preeminent reference model is a male one[7] since it is theoretical and does not ponder intuitive and emotional factors generally attributed to female thinking and aptitudes[8]. Moreover gender biases are even more evident in relation to technological knowledge: this research field has always been considered a preferred one for a predominantly male presence, as opposed to a female component that is not sufficiently ready to acquire technological skills and abilities[9]. This has fostered a vision that is no longer only factual but also perpetuated in the digital context in favor stereotypical and prejudicial social models of the female role and image, especially when they refer to limited opportunities for women and girls to participate in and contribute to the development of technological knowledge related to artificial intelligence[10].

More specifically, gender biases are a category to be further carefully explored calling for the above mentioned need for a proper comprehensive legal framework: they can be produced either in the process of setting algorithms through the use of word embeddings in the programming language that contain sexist formulas, or in data collection and storage even as it relates to the monitoring and evaluation of results of such activities - since they can incentivize a discriminatory appraisal based on factors such as gender, age, ethnic origin, religion, political or sexual orientation, or even in decision-making on the basis of the artificial intelligence programs in place[11]. It is precisely at these stages, with particular emphasis placed on the latter one, that the no gender-neutral consideration about knowledge and application of digital technologies clearly emerges.

In fact, structural and operational disparities related to the lack of the gender component in science and technology fields result in the design and implementation of appli-

[7] H. Schelhowe, *Paradigms of computing science: The necessity for methodological diversity*, in *Gender, Technology and Development*, 8, 2004, 321 ss.

[8] D.M. Sutko, *Theorizing femininity in artificial intelligence: a framework for undoing technology's gender troubles*, in *Cultural Studies*, 34, 2020, 567 ss.

[9] D. Johnson, *Sorting out the Question of Feminist Technology*, University of Illinois, 2010.

[10] A.R. Fryxell, *Artificial Eye: The Modernist Origins of AI's Gender Problem*, in *Discourse*, 43, 2021, 31 ss.

[11] A. Manasi, *Addressing Gender Bias to Achieve Ethical AI*, IPI Global Observatory, 2023.

cation of artificial intelligence-based programs and systems that are at all gender-neutral. The limited presence of the female component in ICTs-related fields is for sure a consequence of the not at all gender-inclusive approach to human capital - in the face of a growing female percentage in STEM disciplines[12] - and the allocation, according to traditional norms, of care commitments to women and girls, this implying fewer opportunities to access professional careers in ICTs.

The need to incentivize a gender appraisal with respect to ICTs and, in particular, to programs and systems based on artificial intelligence, arose visibly during a debate promoted by UNESCO in 2020 dedicated to the relationship between gender equality and artificial intelligence, for an interpretation designed to promote the definition of principles and legal instruments inspired by an ethical approach aimed at preventing and countering any form of gender discrimination in the digital field.

In this framework the ethical factor takes on a proper connotation: in general, linked to artificial intelligence, it is instrumental for a clear distinction between the human being and the machine: oftentimes, artificial intelligence programs and systems are seen as tools to overcome this distinction on the basis of the large volume of data to be collected, managed, and analyzed - a difficult task for the human mind and, at the same time, artificially solvable through a series of complex machine functions – including also developmental potential and operational flexibility of artificial intelligence[13], which seems quite objective and able of introducing social biases[14].

As above reported, in relation to an ongoing process to negotiate hard standards at the EU/Council of Europe level, in the larger debate promoted at UNESCO[15], since the adoption on November 24, 2021 of the Recommendation on the Ethics of Artificial Intelligence, the active involvement and reception of female contribution in the definition and implementation of a set of ethical principles for the elaboration of artificial intelligence-based programs and systems has been considered crucial. In this sense, the expression ethics by design has been introduced: the dual function of regulation through standards and design of artificial intelligence mechanisms inspired first and foremost by respect for human rights in terms of autonomy, dignity, and freedom, with specific reference to the right to privacy and protection of personal data. Ethics is also essential for the operation of the aforementioned programs and systems in such a way that everyone has equal access to them, enjoying equal rights and equal opportunities, and feels protected as individuals or members of a community, albeit a digital one. Programs and systems, ethically, must be made transparent and accessible

[12] E. Davila Dos Santos - A. Albahari - S. Díaz - E.C. De Freitas, *Science and Technology as Feminine': Raising awareness about and reducing the gender gap in STEM careers*, in *Journal of Gender Studies*, 31, 2022, 505 ss.

[13] A. Gilli - M. Pellegrino - R. Kelly, *Intelligent machines and the growing importance of ethics*, in A. Gilli (ed.), *The brain and the processor: Unpacking the challenges of human-machine interaction*, NATO Defense College, 2019, 45 ss.

[14] R. Benjamin, *Race after technology: Abolitionist tools for the new JIM code*, in *Social Forces*, 98, 2020, 1 ss.; *contra* the idea of flexibility, translated into clarity of purpose and choice, undoubtedly attributable to the human being and not to the machine see above, note 13.

[15] L. Hogenhout, *A Framework for Ethical AI at the United Nations*, UN Office for Information and Communications Technology, Unite Paper, 2021(1).

so that all digital users can know their design and application as well as verify their functioning by assigning specific responsibility to designers if it does not comply with ethical principles. So far ethics by design is indispensable for the compliance with these principles, as a key operational prerequisite for artificial intelligence-based programs and systems and also for the future compilation of dedicated legally binding instruments – moving from the regional to the global level.

For the ethical principles on which the design process rests to be concretely validated, the functioning of any program or system based upon artificial intelligence requires: the predetermination of objectives; the definition of technical and non-technical requirements; a complex design that is nevertheless qualitatively such as to ensure compliance with principles; the operation of data collection, storage and management for its integrity and reliability; the possible development of additional design elements, sufficiently flexible and adaptable to the model; and interventions to verify and evaluate the program or system during its functioning.

While these elements may appear to be primarily technical or otherwise abstract, the specific relevance of the ethical component emerges, even from a gender perspective, when the artificial intelligence-based program or system is able to operate in full compliance with them through the cognitive contribution of the female component to its design and proper functioning.

2. Recommending a gender-based approach in the digital space

The elaboration of digital tools, including those based on artificial intelligence, that are truly gender-neutral is a topic addressed in the United Nations framework to promote a process of legal regulation supported by both member states and actors of a non-institutional nature, particularly ICTs' companies. This process is yet framed along the lines of soft law documents, due to the legal fatigue and eventual barriers for a global support for a dedicated binding treaty over digital issues at large from States but also to the need for a motivated inclusion of private actors to provide their contributions and to accept their 'compliance' to hard standards.

In the most recent considerations shared by the Secretary-General anticipating the 67th session of the Commission on the Status of Women in 2023[16], it is suggested that the compilation of voluntary ethical standards could be a starting point for such a process: they will be able to identify conducts and activities of digital actors as producers of programs and systems so that they are instrumental to both the development and proper functioning of technological tools, particularly those based on artificial intelligence.

In order to ensure the effective impact of these ethically-driven voluntary standards, it will be essential to correlate them with monitoring and evaluation procedures that

[16] For further details see UN, Commission on the Status of Women, Sixty-seventh session, *Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls,* Report of the Secretary-General. E/CN.6/2023/3, 30 December 2022.

cannot be internal to digital actors' frameworks (especially if private) as they could not sufficiently guarantee independent assessments, nor external since they cannot quickly activate the removal of digital content that does not meet the standards or decisively affect ethics by design to correct digital contents.

However, as for the development of digital technologies, a further regulatory step can be shaped, as in the European context, by providing for the compilation of a binding legal framework by digital actors so that: any content that does not comply with it is removed, due diligence is introduced to prevent and manage any risks arising from technological devices to the detriment of users - also from a gender perspective, transparency is ensured in the sharing of information from programs and systems based on artificial intelligence, and moderation methodologies are used about digital contents.

The ultimate goal of this process lies in the introduction and implementation of mandatory standards, defining in a timely manner obligations and responsibilities on digital actors, including the attention paid to the truly gender-neutral dimension of ICTs. It is precisely the volume of digital data that presents, along a gender perspective, limited quantitative relevance as users suffer from an obvious gender digital divide as well as unequal to other categories for processing the same data in disaggregated form. These two factors affect the functioning of artificial intelligence-based programs and systems, making cognitive biases permanent, compressing the quality of digital services, and incentivizing discriminatory appraisal of data.

With particular reference, once again, to the ethical component of programs and systems based on artificial intelligence, it is usual to recall benefits and criticalities produced by different types of biases, including gender biases[17]. The latter, in particular, depend on transferring prejudicial behaviors and stereotype-based conducts from factual to virtual reality and are produced by the limited female promotion and access to STEM disciplines, digital careers and the opportunity to enter technical teams designing automated or artificial intelligence-based technological tools.

The digital gender divide encompasses all forms of obstacles in accessing and attending educational and training paths - from the primary level up to the academic and postgraduate specialization ones - dedicated to technologies and in gaining cultural and social experience about concrete limitations of developing knowledge and skills in order to benefit from the progress stemming from digital transformation and innovation, available through all devices - from smartphones to laptops and access to the web.

The primary consequence of this consideration are concrete limited opportunities for women and girls as scientific or entrepreneurial components or team-leaders to enter the professional field of new digital technologies, and to experiment in the sub-sector of artificial intelligence. Thus, there is not only a segregation of a horizontal nature, if statistical data confirm digital educational and professional disparity between men and women, but also a segregation of a vertical nature related to overcoming the main ob-

[17] E. Lamm - G. Ramos - E. Ronchi - M. Squicciarini, *The Gendered Impacts of AI: Policies and Safeguards to Regulate New Technologies, Mitigate Risks and Protect Rights*. UN Women, Expert Group Meeting 'Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls', 10-13 October 2022.

stacle of access to the digital sector, that is the concrete overcoming the glass ceiling by reaching top positions in the tech sector. In addition to these observations, there is also an additional risk for female workers in the labor market: due to their compressed representation, they could suffer a further form of exclusion resulting from the wider use of automated production mechanisms that will mainly affect professional figures with low and medium levels of education and skills.

3. Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls

While the issue under consideration has been addressed in the United Nations system through a comprehensive analysis of the evolution of the digital sector and the need to introduce regulatory measures of both a voluntary and mandatory nature to prevent and manage different types of biases of artificial intelligence-based programs and systems, specific attention was paid to the gender dimension on the occasion of the 67th session of the United Nations Commission on the Status of Women, held in March 2023 in New York.

The annual session of the Commission requires the predetermination of the so called priority theme, on which debates will be scheduled, including the political and high-level level as well as in technical and interactive format and the dialogue with civil society organizations, which are called upon to provide their input in the framework of informal events and meetings.

The priority theme of the 67th session of the Commission focused on innovation and evolution of technologies, linked to education in the digital age with the goal of achieving gender equality and empowerment of all women and girls.

In the document adopted at the end of the session, the so-called Agreed Conclusions[18], which does not have a binding nature and yet contains interesting recommendations addressed to member states as well as all non-institutional actors who are affected by the issues examined and discussed by the Commission, the priority theme is articulated in its general scope and in order to propose an appraisal that, in the case under consideration, also drew attention to the nexus between gender and artificial intelligence.

In the preambular section of the Agreed Conclusions, the Commission notes the continuity of the gender discriminatory approach and the creation of biases by moving from the real to the virtual context: biases, specifically, are produced by the use of algorithms in artificial intelligence-based programs and systems.

While it is true that such programs and systems have had an important and positive impact in the configuration and activation of new public services, in economic pro-

[18] See UN, Commission on the Status of Women, Sixty-seventh session. Agreed Conclusions. 20 March 2023. Indeed the Agreed Conclusions could be considered as a legal starting point official document to promote the compilation of other relevant UN legal documents, which have a recommendatory relevance or could be retained as a key-tool to encourage the negotiation of legally binding legal instruments.

gress and for collective and extensive social welfare, and in the readjustment of work settings especially during and after the pandemic emergency, at the same time there have been and will continue to be negative consequences on the personal and professional lives of women and girls.

To counter this trend, appropriate emphasis must be placed on efforts to overcome structural and systemic cultural and societal stereotypes and biases that slow down women's and girls' access to STEM disciplines and digital careers. Their presence as female researchers, innovators and entrepreneurs, members and leaders of teams created in the public and private sectors in the digital field is an essential precondition to bring their contributions, in terms of knowledge and experience in the sub-sectors of artificial intelligence, software programming, cloud computing platforms, and data management. The design, development, and application of digital technologies that rest on the neutral and objective collection, storage, and management of data needs such input in order to prevent technical malfunctions and biases inherent in algorithms since the setting of collecting and analyzing data is not really neutral along the gender perspective.

These considerations have been translated into recommendations to the attention of all stakeholders, both public and private, in the operational section of the Agreed Conclusions. In this regard, the adoption of public policies aimed at promoting gender equality and equal opportunity in STEM disciplines is essential to encourage women and girls on their path to employment and professional growth. At the same time, private actors are recommended to adopt technological investment methodologies that give due consideration to preventing and countering discriminatory behaviors and conducts produced by programs and systems based on artificial intelligence, predictive algorithms, and robotics. Finally, a common recommendation addressed to both public and private actors is aimed at adopting measures to regulate and evaluate basic requirements underlying the aforementioned programs and systems for the better prevention and management of gender biases.

Indeed, these considerations are echoed in the aforementioned Recommendation adopted at UNESCO on the Ethics of Artificial Intelligence[19], which can thus be considered a relevant tool for the compilation of useful standards to favour the adoption of a gender-responsive approach to artificial intelligence as a key-precondition towards the elaboration and compilation of dedicated hard standards. In fact in principle automated mechanisms have a potentially discriminatory impact if they are not designed technologically in an appropriate way: the resulting consequences pervade the social sphere and the female component both in positive terms - for example increasing educational knowledge in digital matters, flexible work solutions, acquisition of knowledge for access to financial resources – as well as in negative terms as for labour and wage management and for the highest risk of exposure to all forms of real and virtual violence and harassment over women and girls as key-victims.

The gender dimension is addressed in Policy Area 6 of the document, whose recommendations to member states focus on the need to ensure that digital technologies in

[19] UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 24 November 2021; see also UNESCO, *Artificial intelligence and gender equality*, 2020.

a broad sense, and artificial intelligence specifically, in the duty cycle of programs and systems that rely on it, are instrumental in promoting gender equality.
The governmental authorities are first and foremost required to allocate adequate financial resources in favor of the female population, within the framework of appropriate strategic plans dedicated to the digital topic and the use of related technologies, in support of interventions in the educational and professional sectors.
From a social point of view, in a participatory view by the female component in the definition of policies to overcoming gender gaps, it is important to incentivize the presence and contribution of women and girls in digital teams, both as components and leaders, so that ethics by digital design incorporates the gender factor in an appropriate way for the functioning of programs and systems based on artificial intelligence. Such participatory involvement is instrumental for the prevention and management of gender biases, thus relying on technological knowledge and skills to overcome educational and professional stereotypes and biases effectively and systematically.
Public-private collaboration is also central in the Recommendation, with the goal of identifying and technologically removing gender biases produced by artificial intelligence-based programs and systems when they not only alter the recognition and acceptance of gender diversity but also when they seriously endanger women and girls in the virtual context. This echoes the need, identified at the regional level in the Council of Europe reasoning towards the compilation of a legally binding instrument over AI and algorithms, for an enhanced dialogue and collaboration between public institutions – as rulers – and private companies – as digital technicians – to prevent discriminatory and gender biases through targeted policies and related positive actions.
Finally, member states are urged to encourage the female component in the private sector engaged in the development of digital technologies, facilitating her entry into this male-dominated professional career and subsequent advancement to top positions, and supporting her in accessing financial incentives for this purpose.

4. Towards an AI hard standard setting to preventing and countering discrimination and fostering gender equality

In a complementary view to the UN framework, where the digital topics been translated into potential voluntary rules and standards, even when formulated as recommendations addressed to member states, at the regional intergovernmental level main steps have been promoted towards the compilation of norms specifically devoted to artificial intelligence, appropriately recalling the relevance of the gender component and digital gender biases.
As above recalled, in the Council of Europe, the topic has been debated since May 2019 when the Commissioner for Human Rights adopted a document of a recommendatory nature to the attention of the membership to define the nexus between artificial intelligence and human rights[20]: this document has had the aim not only of

[20] Council of Europe, Commissioner for Human Rights, *Unboxing artificial intelligence: 10 steps to protect*

incentivizing the development of artificial intelligence-based programs and systems but also of preventing or mitigating the negative impact they may have on individual and collective life and rights and freedoms.
In order for this complex goal to be satisfactorily achieved, public stakeholders acquiring, developing, and applying artificial intelligence-based programs and systems are urged to introduce procedures to assess their impact on human rights, to ensure broad and transparent information on the ways through which programs and systems are designed, and to regulate in a timely manner the legislative system that enables them to carry out independent and effective control over the development, dissemination, and use of programs and systems by both public and private actors in terms of their impact on the protection of human rights.
The relevance of the topic led to an important step, namely the creation of a special committee (Ad Hoc Committee on Artificial Intelligence - CAHAI) that exercised its mandate from 2019 to 2021 with the main purpose of testing the possibility of compiling a dedicated binding legal instrument, carrying out a series of multi-stakeholder consultations and producing interesting background papers.
CAHAI has reasoned on the basis of multiple legal standards: first, those of binding and non-binding legal scope adopted in the Council of Europe and appropriately related to the process of design, development and application of digital technologies with respect to the protection of human rights, democracy and the rule of law as fundamental pillars of the Organization since its establishment in 1949; then additional legal instruments of binding and non-binding scope adopted in other intergovernmental global and regional systems. In exercising its mandate, again, CAHAI has paid special attention to the gender dimension.
In an early study paper[21], the Ad Hoc Committee placed the nexus between gender and artificial intelligence in the broader context of promoting principles of equality, non-discrimination and solidarity, specifically emphasizing the scope of the provisions of the European Convention for the Protection of Human Rights and Fundamental Freedoms with reference to Article 14 and its Protocol No. 12, focused on the principle of non-discrimination, albeit gender-based.
Artificial intelligence-based programs and systems have perpetuated and increased discriminatory conducts and behaviours from the real to the virtual context, limiting its monitoring and control and incentivizing biases, regardless of whether produced by mere technological error or consciously and intentionally by the designers of artificial intelligence systems, thus confirming that AI-design is neither neutral nor ethical. The presence and technical contribution of the female component in the design teams of these systems is essential to prevent and manage biases, in the form of multiple discriminations up to violence and harassment against women and girls.
Complementing these remarks of CAHAI, in order to give an overview of binding and non-binding international and regional instruments in force, the opportunity to

human rights, 2019.

[21] Council of Europe, *Towards regulation of AI systems. Global perspectives on the development of a legal framework on Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law,* Compilation of contributions DGI (2020) 16.

draft a convention to regulate artificial intelligence-based mechanisms beyond soft standards was explored by some experts who compiled and presented an interesting study paper in 2021, thus offering interesting insights to the attention of the same Ad Hoc Committee in charge for the preparation the feasibility study towards a legal framework on artificial intelligence[22].

Drawing from the extensive production of guidelines and principles for the ethical configuration and application of artificial intelligence-based programs and systems, the experts pointed out that the voluntary or self-regulatory nature was necessary at the outset for a generic, flexible and adaptable as well as reviewable language and yet led to criticisms related to a rhetorical approach and the practical difficulty of introducing ethical foresight into technological mechanisms, especially when automated. Moreover, experts have differentiated the nature of soft laws adopted by Council of Europe bodies - such as recommendations and declarations or of guidelines with input from all stakeholders - or implemented by member states often on the basis of a public-private partnership (guidelines, codes of conduct).

However, given the extreme dynamism of technological knowledge and the high risk of biases produced by limited ethics by design, the chance of either revising existing binding legal instruments in the digital domain or, otherwise, compiling a dedicated binding legal instrument on artificial intelligence were both considered as necessary and viable options in the Council of Europe.

In the former case, several alternatives were envisaged: the compilation of a Protocol to the aforementioned European Convention, binding on the States Parties and potentially impacting on the backlog of the European Court of Human Rights; and the revision of existing binding legal instruments, such as the Budapest Convention on Cybercrime or Convention 108+ on the Management of Personal Data, although the specificity of artificial intelligence-based programs and systems would require an adaptation of the monitoring and verification mechanisms to automated mechanisms that already operate within the framework of such legal frameworks.

In the latter case, two options have been proposed as to the drafting process.

With respect to the option for the drafting of a framework convention that would lay out basic principles and areas of implementation inherent in the design and functioning of artificial intelligence-based programs and systems, it has been appreciated for the rapid evolution of digital knowledge and technological tools and ethical challenges; a framework convention, however, could leave room for the states parties in terms of obligations for its implementation, possibly framed through additional protocols.

The option for the drafting of a convention would undoubtedly ensure the elaboration of a detailed legal discipline, formulating rights and obligations that could be perceived as too inflexible with respect to technological and digital dynamics and also in terms of domestic legal compliance.

The latter option has been accommodated by the membership of the Council of Europe, promoting this process through the creation, in place of the CAHAI, of the Committee on Artificial Intelligence (CAI), tasked with the compilation of the afore-

[22] D. Leslie - C. Burr - M. Aitken - J. Cowls - M. Katell - M. Briggs, *Artificial intelligence, human rights, democracy, and the rule of law. A primer*, The Alan Turing Institute, 2021.

mentioned binding legal instrument by November 2023.
Indeed, the CAI has worked in line with the document produced by CAHAI at the end of its mandate[23] in which a number of elements have been proposed to underpin the drafting of this new convention.
Indeed, in the document adopted by CAI in 2023, to be considered as the preliminary text of the future Artificial Intelligence Convention[24], an analysis focused on the gender dimension is proposed.
CAHAI had already planned to include a gender reference in the provision concerning the guarantee of equal treatment and respect for the principle of non-discrimination with regard to the design, development and application of systems based on artificial intelligence; for a specific management of gender biases, the Ad Hoc Committee had also noted the opportunity to draft additional provisions concerning specific categories of subjects, including women and girls, who are directly affected by artificial intelligence mechanisms and who, for this reason, must be able to participate in the elaboration of monitoring and control procedures regarding their proper functioning.
The CAI incorporated these indications and formulated the principle of non-discrimination (as of today, Art. 3), introducing factors that artificial intelligence-based systems could entail to operate with discriminatory impact: «sex, gender, sexual orientation, race, color, language, age, religion, political or any other opinion, national or social origin, association with a national minority, property, birth, state of health, disability or other status, or based on a combination of one or more of these grounds».
An additional reference of this principle is included in Art. 12, concerning equality and anti-discrimination, which provides for an obligation on States Parties to ensure that «the design, development and application of artificial intelligence systems respect the principle of equality, including gender equality and rights related to discriminated groups and individuals in vulnerable situations».
In conclusion, apart from a different but complementary approach in dealing with this topic in intergovernmental global and regional systems, it is quite clear the relevance of the issue of gender biases produced by artificial intelligence-based programs and systems and the need to seize this opportunity for drafting legally binding instruments beside soft laws as a further step to ensure the adoption and implementation of hard regulations in this matter.

[23] As mentioned above Council of Europe, *Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law*, 2021.

[24] Council of Europe, *Revised zero draft [framework] convention on artificial intelligence, human rights, democracy and the rule of law*, 2023.

Legal Identity between Artificial Intelligence and the Rule of Law*

Domitilla Vanni

Abstract

The present research will address the complex purpose of providing legal identity, included in the Sustainable Development Goal 16 which concerns "peace, justice and strong institutions" in connection with the wide issue of Artificial Intelligence. Furthermore, in a wider perspective the relevance of the principle of the rule of law also in this field must be underlined as the rule of law guarantees fundamental rights and values, allows the application of law, and supports an investment-friendly business environment. In this framework the principle of accountability plays a key role in the General Data Protection Regulation (GDPR) (art 25, para. 1): the data controller must account for the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the data processing. In the same way a decisive role to prevent and limit violations of human rights is played by the informed consent as the GDPR requires data controllers to justify the collection and processing of personal data on some lawful bases. Controllers can obtain the consent of data subjects to justify this collection of data, but a number of criteria must be fulfilled before the consent can be valid.

Summary

Keywords

SDGs - legal identity - Artificial Intelligence - accountability - informed consent

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

1. Introduction

The present research would address the complex purpose of providing legal identity, included in the *Sustainable Development Goal 16* which concerns "peace, justice and strong institutions" to «promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels», in connection with the wide issue of Artificial Intelligence. Legal identity implies the child's right to be registered at the birth as prerequisite for the consequential rights to a name and nationality, civil rights and overall the right to access to justice and other social services. Artificial Intelligence can help governments to realize the purposes set by SDG 16 but presents a high level of risk in consideration of the interference between new national or international identification systems with the right to privacy. In this framework the concept of "informed consent", that is central to the ethical collection of data, plays a decisive role to prevent any violation of the human right to respect for private life, as guaranteed by art. 8 of European Convention of Human Rights.
So the introduction of new foundational identification systems and more pervasive requirements for proof of identity, without simultaneously addressing gaps in the legal framework governing the determination of legal status and identity, risks making the problems around proof of legal identity worse rather than better.

2. Legal Identity within SDG 16

Firstly what we intend for legal identity? Legal identity has been defined[1] as the «basic characteristics of an individual's identity, e.g. name, sex, place and date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth». In the absence of birth registration, legal identity may be conferred by a legally-recognized identification authority. This system should be linked to the civil registration system to ensure a holistic approach to legal identity. This definition seems to understand legal identity as something to be "conferred by" official authorities issuing birth certificates, identification documents, and civil status documentation[2]. The existence of divergent approaches to the term legal identity highlights the complexity of current policy discussions surrounding SDG 16.9. Most particularly, it highlights the need to critically engage with the way in which different aspects of "legal identity" play out in different situations, particularly complex environments where official authorities may be absent,

[1] * The essay reproduces with updates the paper presented by the Autor in 2022 (28 March) Teams Conference on *Artificial Intelligence and The Rule of Law: A Focus on Sdg 16* organized by the Centre for Law & Development of Qatar University College of Law and the American Society of International Law.
So defined in 2019 by the members of the United Nations Legal Identity Expert group who approved an operational definition of "legal identity".

[2] K. M. A. Fortin, *To be or not to be? Legal Identity in Crisis in Non-international Armed Conflicts*, in *Human Rights Quarterly*, 43, 1, 2021, 29 ss.

especially in emergency situations, as in wars or in pandemics.

The importance of obtaining a legal identity[3] can be underlined on different levels, as establishing a legal identity is crucial for people to access many rights, it is also a basic prerequisite for establishing a nationality and for governments to surveil their populations.

If individuals can show who they are, they will have a greater chance of accessing the systems of social welfare and economic empowerment that are at the heart of the other SDGs. Yet from an international law perspective, the term legal identity in SDG 16.9 seems more naturally to refer to legal personhood, which raises different issues to the mere identification of individuals. A human rights approach to the term legal identity understands it even more broadly, as encompassing not only legal personhood in a binary sense (i.e. to have legal personhood or not) but also the multi-dimensional ways in which legal identity is constructed and threatened, for example by an individual relationship, identificating with, or disassociating from, certain societal groups. Researchers adopting this approach have defined legal identity as a «set of elements and characteristics, the combination of which is unique to every person, which defines each person and governs their relationships, obligations and rights under both private and public law».

As enshrined in art. 6 of the Universal Declaration on Human Rights[4] and in art. 16 of the International Covenant on Civil and Political Rights[5] everyone has the right to be recognized as a person before the law. Several international rules, such as art. 7 of the Convention on the Rights of the Child[6] and art. 24, para. 2, of the International Covenant on Civil and Political Rights[7] also recognized a right to birth registration.

Now Sustainable Development Goal Target 16.9[8], which aimes for: «legal identity for all, including birth registration, by 2030», is the key to advance the 2030 Agenda commitment to leave no one behind, and equally relevant is SDG 17.19 – support

---

[3] A. Heather, *Nomads and the Struggle for a Legal Identity*, in *Statelessness & Citizenship Review*, 2(2), 2020, 338 ss.

[4] Universal Declaration of Human Rights, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948) art. 6.

[5] International Covenant on Civil and Political Rights, opened for signature on 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art. 16.

[6] Art. 7 of the Convention on the Rights of the Child states: «1. The child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents.
2. States Parties shall ensure the implementation of these rights in accordance with their national law and their obligations under the relevant international instruments in this field, in particular where the child would otherwise be stateless».

[7] Art. 24 of the International Covenant on Civil and Political Rights states: «1. Every child shall have, without any discrimination as to race, color, sex, language, religion, national or social origin, property or birth, the right to such measures of protection as are required by his status as a minor, on the part of his family, society and the State.
2. Every child shall be registered immediately after birth and shall have a name.
3. Every child has the right to acquire a nationality».

[8] United Nations (2017) Resolution adopted by the General Assembly on 6 July 2017, Work of the Statistical Commission pertaining to the 2030 Agenda for Sustainable Development (A/RES/71/313 Archived 28 November 2020 at the Wayback Machine).

to statistical capacity-building in developing countries – monitored by the indicator «proportion of countries that have achieved 100 per cent birth registration and 80 per cent death registration».
Inspired by the Secretary-General's determination to tackle the global problem of statelessness (affecting more than 10 million people worldwide), but also noting the wider (and larger) issue of lack of legal identity, the Secretary-General's Executive Committee, in January 2018, mandated the Deputy Secretary-General to convene «UN entities to develop, in collaboration with the World Bank Group, a common approach to the broader issue of registration and legal identity [...]». To operationalize the decision of the Executive Committee, an inter-agency coordination mechanism — the UN Legal Identity Agenda Task Force (UNLIATF) — was established from September 2018, where 13 UN agencies, under the chairmanship of UNDP, UNICEF and the UN Department of Economic and Social Affairs, are working together to try to assist Member States to achieve SDG target 16.9.

3. Legal Identity in the ECtHR case law

Beginning from the analysis of the constitutional principles that can serve as a useful guideline for studying effects and range of application of AI, a mandatory step is constituted by the right to privacy ex art. 8 ECHR[9]. With reference to the amount of data in circulation, it can be recalled how our daily activities and the environment that surrounds us present an infinite number of opportunities to steal and disseminate personal data.
To this purpose it can be useful leaving from a European leading case *Sudita Keita v Hungary*[10] of 2020 in which the European Court of Human Rights found a violation of art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), which protects the right to private and family life. The case concerned Mr Sudita Keita, a stateless person whose legal status in Hungary had been uncertain for a period of almost 15 years, with adverse repercussions on his access to healthcare, employment and on the enjoyment of his right to private life in general[11].

[9] Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature 4 November 1950, ETS No. 005 (entered into force 3 September 1953) art 8 ('ECHR'), which states: «1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others».

[10] ECHR, *Sudita Keita v. Hungary*, app. no. 42321/15 (2020); about it see P. Cabral*, Sudita Keita v Hungary - European Court of Human Rights Decision on the Right to Private Life of Stateless Persons*, in *Statelessness & Citizenship REV*, 2, 2020, 324.

[11] Mr Keita is of Somali and Nigerian descent. He was born in 1985 and arrived in Hungary in 2002 without any valid travel documents. Mr Keita submitted a request or refugee status upon his arrival in Hungary. His request was rejected and Mr Keita was issued with an expulsion order in April 2003. The Nigerian embassy in Budapest refused to recognise him as a national and the Hungarian authorities were unable to return him to Somalia during the civil war. Thus, in 2006, he was admitted with a tolerated status and then granted a humanitarian residence permit for two years. It did not seem that

The *Sudita Keita v Hungary* judgment is noteworthy because it follows and strengthens the Court's principles set out in the other landmark case of *Hoti v. Croatia* of 2018[12], providing consistency to a line of caselaw that addresses statelessness as a core issue and aims to extend protection to persons without a nationality. It reiterates that art. 8 ECHR imposes a positive obligation on states to provide an effective and accessible procedure or a combination of procedures enabling the individual concerned to have the issue of their status determined, with due regard to private-life interests.

In its reasoning, the Court reiterated the principles outlined in *Hoti*. It stated that art. 8 protects the right to establish and develops relationships as well as certain aspects of a person's social identity, thus the social ties between a person and the community in which they live are included in the concept of private life. The Court confirmed that the ECHR cannot be interpreted as guaranteeing a right to reside or a particular type of residence permit, nor can the Court decide which status should be granted. However, the national authorities must offer a solution for stateless people in order for them to enjoy their right to private and family life without obstacles. So in some cases, art. 8 may therefore impose on states a positive obligation «to provide an effective and accessible means of protecting the right to respect for private and/or family life», including a domestic remedy allowing the competent authority to deal with the substance of a complaint under the ECHR and grant adequate relief.

Taking into consideration that the applicant had been living in Hungary since 2002, where he undertook training and established a relationship, and that he did not have a recognised status in any other country, the Court accepted that Mr Keita had the right to enjoy private life in Hungary as protected by art. 8. The uncertainty of his residence and migration status for about 15 years resulted in long periods without entitlement to healthcare and employment and caused adverse repercussions on his private life.

Of particular interest is that the Court considered the applicant's statelessness to be an important element of the case. Although the Government did not contest that the Nigerian embassy had refused to recognise Mr Keita as a national, the Court observed that the authorities failed to inform the applicant about the possibility of applying for stateless status after they became aware of Nigeria's refusal. In the examination of whether the domestic authorities complied with their positive obligations under art. 8, the Court followed the same principles adopted in *Sudita Keita* and *Hoti*, suggesting a consistent reasoning for similar cases: assessing the applicant's social ties to the country, establishing that the uncertainty had adverse repercussions on private life,

the authorities had informed him about the possibility of applying for stateless status, as required by national legislation. In 2008, the Hungarian Immigration Authority reviewed his situation and left Mr Keita once again without a recognised status or valid documents and issued him with a deportation order. In 2010, Mr Keita applied for stateless status. However, the national courts considered that his request should be refused on the grounds that the law required applicants to be "lawfully" staying in the country. After lengthy proceedings, the Constitutional Court of Hungary declared in 2015 that the "lawful stay" requirement was unconstitutional and contrary to Hungary's international obligations in light of the 1954 Convention. The requirement was removed and Mr Keita was finally granted stateless status in October 2017, regaining his entitlement to basic healthcare and employment. So the applicant submitted ECtHR that the Hungarian authorities' refusal to regularise his situation had resulted in a violation of arts. 3, 5, 8, 13 and 14 of the ECHR.

[12] ECHR, *Hoti v. Croatia,* ric. 63311/14 (2018).

examining whether there was an effective possibility of regularising legal status and, finally, whether any requirements were imposed that the applicant was unable to fulfil by virtue of his status.
The above mentioned judgment reinforces the idea that the rights protected under the ECHR are not merely theoretical, but must be practical and effective.
Although Hungary had an established statelessness determination procedure, until 2015 it was only accessible to those lawfully staying in the country and, thus, prevented stateless people from effectively accessing protection. The Constitutional Court of Hungary's decision of February 2015 brought the Hungarian procedure into compliance with international norms[13], and the Court's judgment in Sudita Keita reiterated that it is contrary to the principles of the 1954 Convention to impose on stateless individuals requirements that they are unable to fulfil. This is particularly relevant for stateless people who typically face obstacles in accessing documentation, providing evidence and demonstrating ties to a country, as most of them have been living on the margins of a society that refuses to acknowledge their identity. The Court has once again shown that States' obligations towards stateless persons flow from an integrated approach to international law and human rights with due consideration to the EHCR and international legal instruments.

4. Interplay between AI and Legal Identity

4.1 The principle of accountability

On the other side, the term "Artificial Intelligence" is used to describe a set of programs and systems with very different functions and capabilities. In general, the concept of IA includes all systems and programs that involve computers to learn how to perform tasks traditionally performed by humans. That is, artificial intelligence processes the data it receives, identifies models linked to recurring correlations and then creates new models; this allows the system to test various hypotheses and find new solutions without the human input[14].
It has been well said that AI systems operate autonomously, perceive their environment, persist over a prolonged time period, adapt to change, and create and pursue the best expected outcome[15].
Here we focus on those forms of AI capable of operating autonomously, adapting to

[13] Convention Relating to the Status of Stateless Persons, opened for signature 28 September 1954, 360 UNTS 117 (entered into force 6 June 1960) ("1954 Convention"). Art. 1 of the 1954 Convention, which provides the definition of stateless person, does not admit reservations or modifications. The Constitutional Court concluded that this approach was further supported by the fact that the 1954 Convention distinguishes between rights that are accorded only to lawfully staying persons (e.g. right of association, right to work and housing) and rights that are accorded to all stateless persons, demonstrating that the lawful stay condition should not be applied in general.

[14] G. Comandè, *Intelligenza artificiale e responsabilità tra "liability" e "accountability"*, in *Analisi giuridica dell'economia, Studi e discussioni sul diritto dell'impresa,* 1, 2019, 169; A. Quarta - G. Smorto, *Diritto privato dei mercati digitali*, Firenze, 2020, 308 ss.

[15] S. Russell - P. Norvig, *Artificial Intelligence: A Modern Approach*, Hoboken, 2011, 1 ss.

change, creating or pursuing their own goals. This is an evolved notion of AI but not yet comparable to a general AI capable of trying to imitate the human one.
So the strength of AI lies in its ability to learn by human-provided data. This is the key process actually. In this context, the need for a more complete legal protection is peaceful, given that the devastating effects on the security[16] of the individuals referred to and, above all, the invasion into the sphere of privacy resulting from the use of AI are now incontrovertible, especially in the field of legal identity as it refers to the essence of the human beings, because it is the first way to express our own personality. Given that with reference to the European protection of the right to legal identity on the basis of art. 8 ECHR, the same rule represents the link of it with the topic of Artificial Intelligence with whom – as previously seen – we necessarily have to do in the context of data protection, overall in the perspective of the legal protection of victims of AI systems.
Infact it is precisely in the field of data protection that the general principle of accountability has its roots, according to which «a data controller should be accountable for complying with measures which give effects to the principles stated above»[17]. Since then the principle of accountability has been constantly taken up to the 2013 guidelines also with reference to international data flows[18].
Accountability means that the data controller must implement appropriate technical and organisational measures, such as pseudonymisation and data minimisation, in order to protect the rights of data subjects[19].
For this reason, accountability plays a key role in the GDPR (art 25, para. 1, GDPR): the data controller must account for the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying degrees of likelihood and severity to the rights and freedoms of natural persons. In particular, the data controller must ensure that «by default and by default only the personal data necessary for each specific purpose of the processing [...] are processed. In particular, such measures shall ensure that, by default, personal data are not made accessible without the intervention of the individual to an indefinite number of natural persons». In this way, the GDPR strengthens the preventive measures to protect data subjects.
Here, however, the role assigned to this principle by the data protection authorities must be limited with reference to AI.

[16] P. Lin - K. Abney - G. Bekey, *Robot ethics: Mapping the issues for a Mechanized World*, in *Artificial Intelligence,* 2014, 355 ss.

[17] See the 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*

[18] See e.g. 2009 *International Conference of Data Protection and Privacy Commissioners* (Madrid International Standards); 2011 ISO/IEC 29100 - *Information Technology - Security Techniques - Privacy Framework*; 2015 APEC *Privacy Framework*, in which the multiplicity of tools that can be used for *accountability* purposes is underlined.

[19] J. Alhadeff et al., *The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions*, in D. Guagnin et al eds, *Managing Privacy through Accountability*, London, 2012, 49 ss.; K. Demetzou, *Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation*, in *Computer Law & Security Review*, 35, 2019, 6.

In this perspective on 23rd October 2018 the 40th International Conference of Data Protection and Privacy Commissioners, including the European Guarantor (EDPS), made a statement on Ethics and Data Protection in Artificial Intelligence. It provides a «call for common governance principles on artificial intelligence to be established, fostering concerted international efforts in this field, in order to ensure that its development and use take place in accordance with ethics and human values, and respect human dignity». This statement contains significant passages which give the idea of the essential contribution of data to the transformative and destabilizing nature of AI. In this sense, the centrality of personal data is reiterated first «for the formation of automatic learning systems and artificial intelligence» beyond the risks that they contain intrinsic distortions that can lead to decisions that unjustly discriminate against certain individuals or groups, potentially limiting the availability of certain services or content thus interfering with individual rights such as freedom of expression and information or causing the exclusion of persons from certain aspects of personal, social and professional life. Furthermore, it is emphasized that AI-based systems whose decisions cannot be explained raise fundamental issues of accountability not only for the violation of privacy and data protection law, but also for liability in case of errors and damages. The centrality of the accountability principle emerges in limiting the risks and negative effects of AI. In particular, a mention is made to the accountability of all stakeholders towards individuals, supervisory authorities and other third parties, where appropriate, also with the implementation of audits, continuous monitoring, assessment of the impact of AI systems and review periodic of surveillance mechanisms; collective and joint responsibility, which involves the entire chain of actors and stakeholders; the establishment of demonstrable governance processes for all stakeholders, for example based on governance processes of trust towards third parties or the establishment of independent ethics committees[20].

On the level of the relationship between AI, legal identity and the principle of accountability the recent evolution of artificial intelligence powered facial recognition technology[21] can be observed, not only being attractive to the private sector, as it opened new possibilities for public administration, including law enforcement and border management. A considerable increase in accuracy achieved in the past few years has prompted many public authorities to start using, testing or planning the use of facial recognition technologies across the world.

Using facial recognition technology affects a range of fundamental rights. However, there is limited information about the way and extent to which the technology is used by law enforcement, and about the impact of its use on fundamental rights. The lack of comprehensive and publicly available information about the actual use of the technology limits the opportunities to analyse its fundamental rights implications. The fundamental rights implications of using facial recognition technology vary considerably depending on the purpose, context and scope of the use. Some of the fundamental rights implications stem from the technology's lack of accuracy. For example,

[20] G. Comandè, *Intelligenza artificiale e responsabilità tra "liability" e "accountability"*, cit., 187.

[21] M. O'Flaherty, *Facial Recognition Technology and Fundamental Rights*, in *Eur. Data Prot. L. Rev.*, 6, 2020, 170 ss.

facial recognition technology has higher error rates, producing biased results. Particularly it is less accurate when pointed at women, transgender and non-binary people meaning these people have a higher risk of being misidentified, which can ultimately result in discrimination[22].

But, importantly, several fundamental rights concerns would remain even if there were a complete absence of errors. For instance, the way facial images – obtained and used potentially without consent or opportunities to opt out – can have a negative impact on people's dignity. Similarly, the use of facial recognition technology can also have a negative impact on the freedom of assembly and the freedom of expression, if people fear that facial recognition technology is being used to identify them. So the EU Fundamental Rights Agency summarised, in its recent focus paper on the topic[23], multiple aspects which represent the key to consider before deploying such a system in real life applications. Working with new AI-driven technologies in the field of facial recognition technology, which are not yet fully understood and where experience of practical applications is currently limited, requires the involvement of all relevant stakeholders and experts from different disciplines. In light of the constantly developing technology, interferences with fundamental rights are not easy to predict. Close monitoring by independent supervisory bodies of facial recognition developments is therefore essential. Art. 8, para. 3, of the EU Charter of Fundamental Rights on the protection of personal data requires the oversight of data processing by an independent authority.

But what happens if a data controller does not take all appropriate measures? First of all, art. 82, para. 1, of the GDPR establishes that «anyone who has suffered material or non-material damage as a result of a breach of this Regulation shall have the right to obtain compensation for the damage from the controller or processor right away». Therefore, the civil liability of the data controller is one of the regulatory enforcement instruments relating to data protection. This involves compensation measures for the data subject.

However, the European Parliament is aware that data protection has not only an individual dimension, but also a collective one. Data processing, due to the dimensions it has reached in the era of globalization and the use of technologies, including algorithms, can no longer be considered a private relationship between the data controller and the interested party.

For this reason, a public measure is necessary. Administrative sanctions imposed by the Data Protection Authority oblige the data controller to take all appropriate measures to manage the risks associated with the processing. For this reason, art. 21, par. 5, of Italian legislative decree no. 101/2018 expressly establishes that violations of the provisions set out in the provision of the Italian Guarantor are subject to a pecuniary administrative sanction pursuant to art. 83, para. 5, of the GDPR. The latter states that the violation of the fundamental principles for processing, including the

[22] L. Houwing, *Stop the Creep of Biometric Surveillance Technology*, in *Eur. Data Prot. L. Rev.*, 6, 2020, 174 ss.

[23] FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (FRA focus, Publications Office of the European Union, November 2019) in *fra.europa.eu,* accessed 28 February 2020.

conditions for consent, pursuant to art. 9 on the processing of special categories of personal data, including genetic data, are subject to administrative fines of up to 20 million euros or, in the case of a company, up to 4% of the total annual worldwide turnover of the previous financial year, whichever is higher. The pecuniary administrative sanction is a very strong incentive for the data controller to take all measures to implement the GDPR.

4.2. The informed consent

In the European data protection framework a decisive role to prevent and limit violations of human rights is played by the informed consent as the General Data Protection Regulation (GDPR), which entered into force on 25 May 2018, requires data controllers to justify the collection and processing of personal data on one of six lawful bases. Controllers can obtain the consent of data subjects to justify this collection of data, but a number of criteria must be fulfilled before the consent can be valid[24]. Non-binding guidelines issued by the Art. 29 Working Party (WP29), the representative group of each of the data protection authorities from across the EU, break down the concept of a valid consent under the GDPR. The guidelines focus on the changes and provide practical guidance to ensure compliance with the GDPR. The fundamental elements of valid consent are that the consent of the data subject must be (i) freely given, (ii) specific, (iii) informed and (iv) it must constitute an unambiguous indication of the data subject's wishes[25].

[24] According to art. 4 (11) GDPR, "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. According to art. 7, para. 2: «If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language». Therefore, the consent is valid if it is informed and specific for that particular matter.

[25] *Freely given:* the GDPR requires that data subjects be given real choice and control over their ability to consent. If the data subject has no real choice, feels compelled, or will experience negative consequences if they do not consent, the consent will not be valid. If consent is included as part of a set of non-negotiable terms, it will not have been freely given. Neither will it be freely given if consent for many processing operations is "bundled". Separate consent must be given for each processing operation.
Specific: the specific purpose or purposes for processing the data must be determined and made clear to the data subject before valid consent can be obtained. Valid consent cannot be obtained otherwise. New "fresh" consent must be obtained where a controller wishes to use previously collected personal data for an additional purpose. With each separate consent request, controllers should provide specific information about the purpose for processing the data.
Informed: the GDPR requires that consent be informed, and that subjects understand, prior to giving their consent, what they are agreeing to.
The WP29 has indicated that, at least, the necessary details required for consent to be informed are: the controller's identity, the purpose of each of the processing operations for which consent is sought, the type of data collected and used, the existence of a right to withdraw consent, information relating to the automated processing of data, and, where necessary, information regarding the possible risks of data transfers to third countries.
Unambiguous indication of wish: The requirement of an unambiguous indication of the data subject's wishes means that a deliberate action must be taken by the data subject to consent to a particular

The same European Court of justice, called by Tribunal of Bucharest to clear the interpretation to be given to the concept of "freely given, specific and informed" consent under art. 2, lett. h, of Directive 95/46, now replaced by art. 4, par.11, of EU Regulation 2016/679[26], in *Orange Romania* case[27] of November 2020, as already stated in the *Planet*[28] judgment, ruled that - for the purpose of a valid consent - the indication of wishes must be an active behavior and requires the data subject to have a high level of autonomy in deciding whether or not to give consent. The core of the matter is the concept of consent given unequivocally, that implies an active motion or declaration. A "clear affirmative act" means, in fact, that the data subject has deliberately expressed his agreement to that specific processing of personal data[29]. That is, in the Court's opinion the consent plays a crucial role in the EU data protection law and it represents one of the lawful grounds for processing personal data, pursuant to art. 6 GDPR.

Actually consent is not always necessary for the lawfulness of processing some categories of data according to the GDPR. According to art. 6 of the GDPR consent is only one of the legal basis of data processing. For example, consent is an alternative option to the pursuit of the legitimate interest of the data controller.

What about the processing of special categories of personal data, such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data concerning the health or sex life of a natural person orientation? Is consent required for the processing of

processing. This can be obtained through written or (recorded) oral means, or electronically, through an active affirmative motion such as clicking a button on a website's privacy statement. A notable change under the GDPR is that controllers will no longer be allowed to offer pre-ticked boxes, or "opt-out" constructions.

[26] In this context, some clearance is also provided by the European Data Protection Board (hereinafter EDPB) Guidelines 05/2020 on consent under Regulation 2016/67920, adopted on 4 May 2020.

[27] CJEU, C-61/19 *Orange Romania SA v. Autoritatea National de Supraveghere a Prelucrarii Datelor cu Caracter Personal* (ANSPDCP), (2020); about it see E. Kaiser, *The Concept of "Freely Given, Specific and Informed" Consent under the Scrutiny of the European Court of Justice*, in *Eur. Data Prot. L. Rev.*, 6, 2020, 607.

[28] CJEU, C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbande - Verbraucherzentrale Bundesverband v. Planet49 GmbH* (2019).

[29] In the *Orange Romania* case, the consent has been expressed by ticking a specific box on a predefined form, without providing the users with the information regarding the consequences of the denial of the consent. It was therefore practically impossible to determine whether the data subject had unequivocally expressed his wishes with regard to the processing of his data. Furthermore, only internal sales rules of Orange were indicating that the objection to the copy and conservation of the IDs should have been documented in the contract and in handwriting. So the European Court of Justice in that judgement ruled that: a contract which contains a clause stating that the data subject has been informed of, and has consented to, the collection and storage of a copy of his or her identity document, is not such as to demonstrate that the person has validly given his or her consent, if: 1) the box referring to that clause had been ticked by the data controller before the contract was signed; 2) the terms of the contract could mislead the data subject regarding the possibility to conclude the contract also without the consent to that processing of his or her personal data; 3) the freedom to give or refuse the consent has been affected by the fact that the data controller demanded the data subject to fill out an additional form. It lies in any case on the data controller the burden of proof to demonstrate that the data subject has, by an active behavior, given his or her consent to the processing of his or her personal data and that he or she has received all information relating to the processing in an intelligible and easily accessible form, using clear and plain language, allowing him or her to understand the consequences of giving or denying the consent.

these special categories of personal data?
Pursuant to art. 9, para. 1, and para 2.a, GDPR, processing of special personal data is prohibited unless the data subject has given explicit consent to the processing of such personal data for one or more specified purposes. Therefore, consent makes the processing of special data lawful if it is given for specified purposes. However, on a closer inspection, consent is an alternative condition in the processing of special categories of personal data. Art. 9, para. 2, provides that the processing of special categories of personal data is not prohibited if the processing is necessary for the assessment of the processing worker's capacity, medical diagnosis, health or social care or treatment, or the management of health or social care systems and services (see point h); for reasons of public interest in the area of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of health care and medicines or medical devices (see point i); for scientific, research or statistical purposes (point j). If one of these conditions is met, special categories of personal data may also be processed without any form of consent. Therefore, consent is not the only possible legal basis for data processing, according to art. 9.

5. AI and the rule of law

Furthermore, in a wider perspective the relevance of the principle of the rule of law also in this field must be underlined as, following the reflection launched by the *Communication on Further strengthening the Rule of Law within the Union* in April 2019, which set out three pillars for future action – promotion, prevention and response – and invited all stakeholders to contribute to a reflection on the next steps, the European Commission received more than 60 contributions from a broad diversity of contributors, including Member States, EU institutions, international organisations and political actors, the judiciary and judicial networks, civil society organisations, academia and associations. The vast majority of contributions acknowledged the importance of strengthening the rule of law for the future of democracy in Europe and the need to reinforce action at all stages – promotion, prevention and response.
On a European level the rule of law guarantees fundamental rights and values, allows the application of EU law, and supports an investment-friendly business environment. It is one of the fundamental values upon which the EU is based on[30].

[30] The European Rule of Law mechanism provides a process for an annual dialogue between the Commission, the Council and the European Parliament together with Member States as well as national parliaments, civil society and other stakeholders on the rule of law. The Rule of Law Report is the foundation of this new process.
A core objective of the European Rule of Law Mechanism is to stimulate inter-institutional cooperation and encourage all EU institutions to contribute in accordance with their respective institutional roles. This aim reflects a long-standing interest from both the European Parliament and the Council. The Commission also invites national parliaments and national authorities to discuss the report, and encourages other stakeholders at the national and EU level to be involved.
The Rule of Law Report and the preparatory work with Member States takes place annually as part of the Mechanism, and will serve as a basis for discussions in the EU as well as to prevent problems from emerging or deepening further. Identifying challenges as soon as possible and with mutual support from the Commission, other Member States, and stakeholders including the Council of Europe and the

The most comprehensive definition of the rule of law was given in particular by the English jurist Albert Venn Dicey, Vinerian Professor of Common Law of England in the University of Oxford from 1882 to 1909, in his *Introduction to the Study of the Law of the Constitution* of 1885[31].

Dicey believed that two principles were inherent in the non written British constitution. The first, and primary principle, was the "sovereignty or supremacy of Parliament" (thus endorsing the notion of representative government as the main feature of a democratic state). The second principle, which tempered the first, was the rule of law, intended as a constraint of the theoretically unlimited power of the State over the individual. In Dicey's opinion the rule of law principle resulted from the existing common (judge-made) law over the years, and it was not necessary therefore to be codified in any written constitution. For Dicey the rule of law had three core features: firstly no person should be punished but for a breach of the law, which should be certain and prospective, so as to guide people and not to permit them to be punished retrospectively. He believed that discretionary power would lead to arbitrariness. Secondly, no person should be above the law and all individuals should be equally subjected to the law. Thirdly, the rule of law should emanate both from the legislation and from the common (judge-made) law.

The rule of law[32] has been variously interpreted through time, but it must be distinguished from a purely formalistic concept under which any action of a public official, authorised by law, is said to fulfil its requirements. Over time, the essence of the rule of law in some countries was distorted so as to be equivalent to "rule by law", or "rule by the law", or even "law by rules". Perhaps the following recent definition by Tom Bingham[33] covers appropriately the essential elements of the rule of law: «All persons and authorities within the State, whether public or private, should be bound by and entitled to the benefit of laws publicly made, taking effect in the future and publicly administered in the Courts». This short definition, which applies to both public and private bodies, is expanded by other "ingredients" of the rule of law. These include: (1) Accessibility of the law (which must be intelligible, clear and predictable); (2) Questions on legal rights should be normally decided by law; (3) Equality before the law; (4) Power must be exercised lawfully, fairly and reasonably; (5) Human rights must be protected; (6) Means must be provided to resolve disputes without undue cost or delay; (7) Trials must be fair, and (8) Compliance by the State with its obligations in international law as well as in national law.

Venice Commission, could help Member States find solutions to safeguard and protect the rule of law.

[31] A. V. Dicey, *Introduction to the Study of the Law of the Constitution*, 1893, 183; A. L .Goodhart, *The Rule of Law and Absolute Sovereignty*, in *University of Pennsylvania Law Review*, 4, 1958, 945; I. Jennings, *The Law and the Constitution*, London, 1952, 47; R. A. Cosgrave, *The rule of law: Albert Venn Dicey, Victorian Jurist*, Chapel Hill, 1980; N. S. Marsh, *The rule of law as a supranational concept,* in A.G. Guest (ed.), *Essays in Jurisprudence*, *A collective work*, London, 1961; W. Lucy, *Abstraction and the Rule of Law*, in *Oxford Journal of Legal Studies*, 2009, 483; M. Serio, *Brevi osservazioni* su *rule of law e sviluppi della teoria di Albert Venn Dicey*, in B. De Donno - F. Pernazza - R. Torino - G. Scarchillo - D. Benincasa (eds.), *Persona e attività economica tra libertà e regola. Scritti dedicati a Diego Corapi,* Naples, 2016, 233 ss.

[32] J. Jowell, *The Rule of Law and its Underlying Values*, *in The Changing Constitution*, J. Jowell - D. Oliver (eds.), Oxford, 2011; E. O. Wennerström, *The Rule of Law and the European Union*, Uppsala, 2007, 61.

[33] T. Bingham, *The Rule of Law,* London, 2010.

The rule of law in its proper sense is an inherent part of any democratic society and the notion of the rule of law requires everyone to be treated by all decision-makers with dignity, equality and rationality and in accordance with the law, and to have the opportunity to challenge decisions before independent and impartial Courts for their unlawfulness, where fair procedures are accorded. The rule of law thus addresses the exercise of power and the relationship between the individual and the State.

The concept of the rule of law can be found at the national as well as at the international level. For Council of Europe, the most important references to the rule of law are found in:

the Preamble to the Statute of the Council of Europe[34], which underlines the "devotion" of member states «to the spiritual and moral values which are the common heritage of their people and the true source of individual freedom, political liberty and the rule of law, principles which form the basis of all genuine democracies»;

the Preamble to the European Convention on Human Rights[35], which states that «the governments of European countries […] are like-minded and have a common heritage of political traditions, ideals, freedom and the rule of law».

In the same perspective the 2018 European Ethical Charter on the use of artificial intelligence in judicial systems and their environment is the first European instrument to set out some substantial and methodological principles which apply to the automated processing of judicial decisions and data, based on AI techniques. Developed by the Council of Europe's European Commission for the Efficiency of Justice (CEPEJ), it is aimed at private companies (start-ups active on the market of new technologies applied to legal services-legaltechs), public actors in charge of designing and deploying AI tools and services in this field, public decision-makers in charge of the legislative or regulatory framework, and the development, audit or use of such tools and services, as well as legal professionals.

At the outset, the CEPEJ points out that the use of AI tools and services in judicial systems is intended to improve the efficiency and quality of justice and deserves to be encouraged. However, it must be done in a responsible manner, respecting the fundamental rights of individuals as set out in the European Convention on Human Rights (ECHR) and in Council of Europe Convention on the Protection of Personal Data[36], as well as the other fundamental principles set out in the Charter.

Among these principles, respect for human rights and non-discrimination is of fundamental importance. The objective is to ensure, from the conception to the practical application, that the solutions ensure respect for the rights guaranteed by the ECHR and the Council of Europe Convention No 108. The principle of non-discrimination is expressly stated because of the ability of certain processing operations – in particular in criminal matters – to reveal an existing discrimination by aggregating or classifying data relating to persons or groups of persons. Public and private actors must therefore

[34] Statute of the Council of Europe, adopted in London on 5 May 1949.

[35] Convention for the Protection of Human Rights and Fundamental Freedoms, adopted by the Council of Europe in Rome on 4 November 1950.

[36] The Council of Europe Convention n°108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

ensure that these applications do not reproduce or aggravate this discrimination and do not lead to deterministic analyses or practices.
Some qualitative challenges related to the analysis methodology and automated processing of court decisions are also taken into account. A principle of quality and security is clearly stated: it should be possible to process data by automatic learning on the basis of certified originals and the integrity of this data should be guaranteed at all stages of processing. The creation of multidisciplinary teams, composed of judges, social science and computer researchers, is strongly recommended, both at the drafting and steering stage and in the application of the proposed solutions.
The principle of transparency of the methodologies and techniques used in the processing of judicial decisions is also of great importance. The emphasis here is on the accessibility and understanding of data processing techniques, as well as on the possibility for authorities or independent experts to carry out external audits. A certification system, to be renewed regularly, is also encouraged.
In addition, the need to make the user an enlightened agent and to feel in charge of his/her choices is stressed. In particular, the judge should be able to return at any time to the judicial decisions and data that have been used to produce a result and continue to have the possibility of departing from it, taking into account the specificities of the case in question. Each user should be informed, in clear and understandable language, of the binding or non-binding nature of the solutions proposed by AI instruments, the various possible options and his or her right to legal advice and recourse before a court.
The CEPEJ hopes that these principles will become a concrete reference point for justice professionals, institutions and for political actors who are faced with the challenge of integrating new AI-based technologies into public policies or into their daily work. In addition, in practical terms, these principles provide an important basis for comparison in assessing the characteristics of the different applications of AI the integration of which into the judicial system or at the court level is now being pursued exponentially.
The CEPEJ is at the disposal of the member States, of judicial institutions and representatives of the legal professions to assist them in the implementation of the principles of the Charter[37].
More recently, the Commission of the European Union made public the proposal for a regulation on 21 April 2021 (*Artificial Intelligence Act*, 'AIA') which represents the first attempt to regulate AI in general terms: it is the result of a preparatory process which has seen, at a European level, the issuing of numerous acts of impulse and soft law in the field of artificial intelligence. Among these, we recall the resolutions of the European Parliament on the ethical principles of AI, robotics and related technology and on the civil liability regime for AI (both of 20 October 2020) and, more recently, on the use of AI (January 20, 2021). Even the Commission's White Paper on Artificial Intelligence (19 February 2020) had already indicated an approach aimed at combining

[37] See the *Document adopted at the 37th plenary meeting of the CEPEJ, Strasbourg and online, 8 and 9 December 2021* by the European Commission for the Efficiency of Justice (CEPEJ) entitled «Revised roadmap for ensuring an appropriate follow-up of the CEPEJ Ethical Charter on the use of artificial intelligence in judicial systems and their environment».

excellence and trust in AI and its general lines were discussed through an intense phase of consultations, which ended in May 2020. A first aspect to consider in describing and evaluating the AIA proposal, therefore, refers to the global context and the relative dynamics in which it is destined to arise. Based on these considerations, a discipline that aims to regulate the AI phenomenon effectively and realistically must be able to accurately balance different interests and conceptions: it must not inhibit AI research and development, encouraging economic investments, at the same time having to affirm and consolidate the principles of the rule of law; it must be flexible and adaptable to the technological changes and rapid development that characterize technology, also ensuring a necessary degree of certainty and predictability for such a strategic and delicate field; it must not be inhibited by possible abuses in the use of AI but it must be able to courageously explore new and beneficial domains, promoting and strengthening the fundamental rights of people and the health of our planet itself. It is a balance that is not easy to strike at a national level, let alone at a European or global level: rules are necessary to ensure respect for the rights and values on which the European Union is based, but they must not cause a disproportionate obstacle compared to the margins of technological, economic and social development that AI can represent.

From the point of view of the chosen instrument, the EU has opted for the adoption of the regulation instead of the directive, in terms similar to what it was done with the GDPR for data protection regulations: its legal basis in art. 114 of the TFEU (which provides for the adoption of measures aimed at ensuring the creation and functioning of the internal market) is thus likely to determine uniform and directly applicable constraints throughout the Union, with the aim of establishing a homogeneous regulatory and tendentially rigid framework for Member States, except for certain margins of maneuver and appreciation for the regulation of *sandboxes* and codes of conduct, for the internal organization of the States and for the sanctioning regime. The attempt to give the EU a uniform and certain framework of rules is accompanied, however, by the need for mechanisms for updating the discipline: AI is, as is known, a difficult object to regulate, both because, even more than other innovative technologies, is characterized by constant developments that quickly render obsolete any discipline aimed at regulating it, both because, in its most advanced systems (machine learning, deep learning, neural networks) it is characterized by a strong dose of autonomy and unpredictability of operation, which, accompanied by the inexplicability of internal processes (black box phenomenon) can represent a potential source of risks, which cannot be calculated ex ante[38]. So the AIA proposal takes into account the plural and diversified nature of AI. Although reduced in unitary terms to any software capable, for a given set of objectives defined by man, of generating outputs (contents, forecasts, recommendations, decisions) that influence the environment with which they interact. AI includes techniques and applications that

[38] M. U. Scherer, *Regulating artificial intelligence systems: risks, challenges, competencies and strategies*, in *Harvard Journal of Law & Technology*, 29, 2016, 365, for whom «one important characteristic of AI that poses a challenge to the legal system relates to the concept foreseeability»; infact, as «AI systems are not inherently limited by the preconceived notions, rules of thumb, and conventional wisdom upon which most human decision-maker rely, AI systems have the capacity to come up with solutions that humans may not have considered, or that they considered and rejected in favor of more intuitively appealing options».

are also very distant, the functioning of which is characterized by variable degrees of autonomy, unpredictability and transparency, and the use of which leads to results, potentialities and risks that are also very varied. In this sense, for example, one thing is to speak generically of expert systems, another thing is about neural networks, characterized by very different trade-offs in terms of autonomy, transparency and explainability. Furthermore, for each AI system, the concrete possibilities of human control are very different. At one extreme are the systems that could perform their functions in complete autonomy (Human out of the loop), at the other those that are governed entirely by humans (Human in command), passing through a series of intermediate positions in which the human dimension plays an increasing role (Human post the loop, Human on the loop and Human in the loop). The proportionate approach to risk control introduced by the AIA proposal is based on the awareness of the aforementioned complexities and of these latter specificities, which translates into a differentiated regulation of AI. In particular, a distinction is made between unacceptable risk systems, for which a prohibition regime is envisaged unless expressly waived, high risk systems, to which most of the regulations are dedicated, low and minimum risk systems, which, substantially free, are subject to information charges only[39].

6. Conclusive remarks

The SDG target 16.9 about legal identity is both an opportunity and a threat for stateless persons or those at risk of statelessness. It is an opportunity as it emphasizes the importance of official recognition and registration as a means for each individual to enjoy civil rights as a member of society; but it is also a threat as the lack of legal protection of stateless or doubtful status people entails the risk the latter will be left behind[40]. Legal identity field is vastly complicated by differences of legal approach between registration systems in the world, especially in developing countries. In this sense the World Bank's *Principles on Identification for Sustainable Development*, endorsed by a wide range of international agencies and private sector actors, include a commitment to non-discrimination, to provide legal identification to all residents, not just citizens[41]. In this framework the spread of new communication and digital technologies is significantly reshaping the operation of identification management systems and contributing to their proliferation. Biometric identifiers are becoming a common feature in identity

[39] About difficulties in definition of AI see S. Russell - P. Norvig, *Artificial Intelligence: A Modern Approach*, Prentice Hall, 2020, 17; B. C. Smith, *The Promise of Artificial Intelligence: Reckoning and Judgment,* MIT press, 2019; B. Marr, *The Key Definitions of Artificial Intelligence (AI) That Explain Its Importance*, in Forbes, February 14, 2018, in //forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its importance/#285881804f5d. See the European Commission High-Level Expert Group on Artificial Intelligence, *A definition of AI: Main Capabilities and Disciplines*, Brussels, April 2019 in //digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines.

[40] B. Manby, *Legal Identity for All' and Statelessness: opportunity and threat at the junction of Public and Private International Law*, in *Statelessness & Citizenship Rev*, 2, 2020, 271.

[41] *Principles on Identification for Sustainable Development: Toward the Digital Age* (Principles, World Bank 2018) 8.

verification and authentication[42]. More and more developing countries have integrated biometrics into their identification management systems[43].

The significant growth in available digital data and the double public-private nature of many identification systems highlighted the great risks linked to data protection, privacy rights, abuse for surveillance purpose, etc. These risks are emphasized in developing countries where institutional capacities, rule of law and accountability might be weak.

So despite artificial intelligence systems in the legal identity field can represent an appropriate remedy against statelessness, however, the lack of adequate regulation on the development and deployment of AI-powered technology poses a serious threat to our human rights law. In Europe, we have already seen the negative impact of AI when it is mismanaged. For example, the discriminatory use of AI at the border has facilitated the deportation of people denying them access to vital services such as health care and social security. We also saw how the use of predictive policing systems led to a dangerous increase in the over-policing of racial communities, and how poor, working-class and immigrant areas have been unfairly targeted by fraud detection systems. The use of facial recognition and similar systems have been used across Europe in ways that lead to mass biometric surveillance.

By fostering mass surveillance and amplifying some of the deepest social inequalities and power imbalances, AI systems are putting our fundamental rights and democratic processes and values at great risk. That is why a proposal by the European Union (EU) institutions on this issue is a globally significant step although the structural, social, political and economic impacts of using AI still must be addressed.

Conclusively, the fast development of new technologies compares humanity with enormous problems and fears. Will there be any space for human contribution in a world of work dominated by increasingly intelligent machines? How will we be able to defend ourselves from the subtle and pervasive dynamics of artificial intelligence systems and at the same time not to give up on intelligent monitoring aimed at our security? What would it happen to areas such as education or justice or healthcare if they were managed exclusively by algorithms? What new rules will have to be applied so that the digital revolution, with the extraordinary possibilities of growth and development that it entails, does not turn into a trap for our species? Robotic systems and artificial intelligence must complement professionals, not replace them; they must not counterfeit humanity, favoring the false idea that those who interact with them are relating to a human being; finally, they must always indicate with maximum transparency the identity of their creators, controllers and owners, especially in order to be able to apply – without uncertainty – civil liability rules for enabling compensation for damages.

---

[42] B. Ajana, *Biometric Citizenship*, in *Citizenship Studies*, 7, 2012, 861; P. Pointner, *Hybrid Tech: The Future of Biometric ID Verification?*, in *Biometric Technology Today*, 8, 2017.

[43] As India's Aadhaar system which uses biometric identifiers for the roll-out of the world's most ambitious foundational identification programme. It has been used as a model for proponents of technological solutions to legal identity problems who often cite it as a proof for the feasibility of implementing large-scale digital identification programmes in developing countries.

Procedimento penale e diffusione dei dati personali. Stato dell'arte e quesiti posti dalla riforma Cartabia*

Andrea Tigrino

Abstract

L'articolo intende affrontare il tema della tutela della riservatezza in relazione ai procedimenti penali, principiando dalla disciplina in materia di anonimizzazione dei provvedimenti giurisdizionali e successivamente esaminando l'annosa questione del diritto all'oblio, da cui un occhio di riguardo alla più recente giurisprudenza interna e sovranazionale. Infine, alcune considerazioni conclusive sono riservate ai profili di maggior rilievo della Riforma Cartabia, che al diritto in parola ha dedicato il nuovo art. 64-*ter* disp. att. c.p.p.

The article aims to address the issue of the right to privacy in relation to criminal proceedings, starting from the provisions on the anonymisation of judicial decisions and then examining the age-old question of the right to be forgotten, hence an eye to the most recent national and supranational jurisprudence. Finally, some concluding remarks are reserved for the most important aspects of the Cartabia Reform, specifically the new article 64-*ter* disp. att. c.p.p.

Sommario

Keywords

provvedimenti giurisdizionali – oblio – deindicizzazione – giurisprudenza sovranazionale – Riforma Cartabia

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

1. Introduzione. La tutela dei diritti fondamentali e del diritto alla privacy in relazione alla circolazione di dati personali acquisiti nel corso di procedimenti penali

La tutela della riservatezza è tema di capitale importanza nella storia del processo penale, considerato come i limiti imposti all'accesso a specifici documenti e atti processuali siano tesi ad assicurare alcune irrinunciabili garanzie: fra di esse, basti pensare all'obbligo di segreto riguardante gli atti di indagine (art. 329 c.p.p.), imposto a fronte della necessità investigativa di scongiurare l'inquinamento o la perdita di elementi di prova, nonché anzitutto all'art. 114 c.p.p., che al suo c. 5 consente al giudice, sentite le parti, di «disporre il divieto di pubblicazione di atti o di parte di atti quando la pubblicazione di essi può offendere il buon costume o comportare la diffusione di notizie sulle quali la legge prescrive di mantenere il segreto nell'interesse dello Stato ovvero causare pregiudizio alla riservatezza dei testimoni o delle parti private» (divieto cui non deroga nemmeno il disposto dell'art. 116 c.p.p., il quale, nel disciplinare il rilascio di copie, estratti e certificati di singoli atti, esplicita al suo c. 3 come il rilascio stesso non faccia venir meno il divieto stabilito dall'art. 114 c.p.p.)[1].

Ponderati i numerosi punti di contatto fra diritto penale e privacy diffusamente affrontati nel corso degli ultimi anni (si pensi al tema della *data retention*[2] e alle riflessioni svolte a proposito della fattispecie di "diffusione illecita di immagini o video sessualmente espliciti" *ex* art. 612-*ter* c.p., recentemente introdotta dalla l. 19 luglio 2019, n. 69[3]), il profilo che il presente contributo intende approfondire attiene alla tutela della riservatezza – e, congiuntamente, di diritti fondamentali quali la dignità – dell'indagato e dell'imputato attraverso l'epurazione di dati personali contenuti in provvedimenti giurisdizionali o diffusi nell'ambito della cronaca giornalistica, focalizzando così l'attenzione tanto su di un contesto cronologico contestuale alla definizione del giudizio, quanto anche di molto successivo alla commissione e alla valutazione dei fatti conte-

[1] Una riflessione sui rapporti fra diritto alla riservatezza e processo penale all'indomani dell'approvazione del d.lgs. 30 giugno 2003, n. 196 è reperibile in C. Oleari, *Articolo 52. Dati identificativi degli interessati*, in *Codice della* privacy, Milano, 2004, 1, 774 ss., con particolare riferimento al par. 2.1 e all'ampia digressione inerente alle disposizioni del Codice di rito riservate al regime pubblicitario degli atti posti in essere nel corso delle diverse fasi del procedimento. Con specifico riguardo a quella delle indagini preliminari, più recentemente M. Torre, *Privacy e indagini penali*, Milano, 2020. Per una raccolta di alcuni importanti provvedimenti del Garante *privacy* inerenti al rapporto fra cronaca e giustizia penale (pubblicazione di inviti a comparire, richieste di rinvio a giudizio e atti d'indagine, diffusione di intercettazioni, foto segnaletiche e notizie riguardanti le vittime di reato, ecc.), vedasi già M. Paissan (a cura di), *Privacy e giornalismo. Diritto di cronaca e diritti dei cittadini*, Roma, 1ª ed., novembre 2003, par. 8, nonché la 2ª ed. agg., 2008, par. 7.

[2] Fra le opere monografiche in materia, si segnalano quelle di G. Formici, *La disciplina della* data retention *tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, Torino, 2021, in particolare il Cap. I e i riferimenti alla lotta alla criminalità e al terrorismo; R. Flor - S. Marcolini, *Dalla* data retention *alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale*, Torino, 2022.

[3] A proposito dell'art. 612-*ter* c.p. e del suo bene giuridico, individuato proprio nella tutela della riservatezza della vittima, v. E. Lo Monte, *L'art. 612-*ter *c.p.: Diffusione illecita di immagini o video sessualmente espliciti: tra buoni propositi, denegato diritto all'oblio e "morti social"*, Torino, 2021; G. M. Palmieri, *L'accoglimento del concetto di "genere" come rischio di una tutela penale a binario differenziato. Art. 612-*ter *c.p. e tutela della riservatezza*, in *Archivio penale*, 2, 2022.

stati. A tal fine, si procederà sia all'esame di norme che vincolano l'operato dell'autorità giudiziaria nell'attività di anonimizzazione dei provvedimenti medesimi (artt. 51 e 52 del d.lgs. 30 giugno 2003, n. 196, Codice in materia dei dati personali), sia di quelle che il soggetto "interessato" può far valere nei confronti del "titolare del trattamento" ai fini della "cancellazione" dei dati che lo riguardano, con ciò facendosi riferimento al tema del diritto all'oblio e all'art. 17 del regolamento (UE) 2016/679 (GDPR, *General Data Protection Regulation*); tale disposizione, pur richiamando espressamente il solo concetto di cancellazione, è stata oggetto di un'approfondita esegesi a opera della giurisprudenza nazionale e sovranazionale, che all'oblio medesimo ha connesso obblighi di aggiornamento, contestualizzazione e "deindicizzazione" dei dati contestati. Il nuovo art. 64-*ter* disp. att. c.p.p., introdotto dalla recentissima Riforma Cartabia al fine di disciplinare il "diritto all'oblio degli imputati e delle persone sottoposte alle indagini", richiama espressamente le disposizioni summenzionate e, appunto, il concetto di deindicizzazione, rendendo così imprescindibile l'approfondimento delle stesse e delle pronunce che a tale posizione giuridica soggettiva hanno dato corpo nel corso dell'ultimo decennio.

Il tema, di particolare complessità interdisciplinare e d'ardua sistematizzazione, è reso ancor più delicato dal necessario bilanciamento di tali istanze con le esigenze di pubblicità connaturali all'amministrazione della giustizia[4] e, conseguentemente, con il diritto di cronaca[5], potendosi in quest'ottica richiamare alcuni fra i numerosi princìpi di matrice nazionale e sovranazionale ivi rilevanti: mentre il connotato di pubblicità viene esaltato anzitutto dall'art. 47 della Carta Fondamentale dei Diritti dell'Unione Europea e dall'art. 6 CEDU, gli artt. 7 e 8 della stessa Convenzione ineriscono rispettivamente alla tutela della vita privata e familiare, del domicilio e delle comunicazioni nonché dei "dati di carattere personale", cui la diffusione di informazioni concernenti un procedimento penale risalente al passato potrebbe chiaramente arrecare un pregiudizio; tuttavia, proprio gli artt. 7 e 8 CEDU devono essere posti in equilibrio con il diritto alla libertà d'espressione garantito dall'art. 10 CEDU, evocato di fronte alla Corte di Strasburgo da parte di ricorrenti responsabili della diffusione mediatica di vicende giudiziarie. In Italia, l'art. 101 Cost. ricorda che «la giustizia è amministrata in nome del popolo», traendosi da ciò un interesse della collettività tanto di carattere attuale (ossia, a essere informata tempestivamente e in maniera esaustiva) quanto rivolto al passato, con ciò alludendosi alla possibilità di effettuare ricerche d'archivio o di essere aggiornati quanto allo sviluppo di procedimenti la cui reviviscenza sia dovuta all'intervento di fattori tali da assicurare agli stessi una rinnovata attualità. Come puntualizzato da un'importante pronuncia della Corte costituzionale, «la pubblicità del giudizio, specie

[4] Per una riflessione sulla pubblicità del processo penale a partire dalla sua natura di *iudicium publicum* nel diritto romano, il rimando è a F. Carnelutti, *La pubblicità nel processo penale*, in *Rivista di diritto processuale*, 1955, 1 ss., scritto in cui l'autorevole dottrina si interroga fra l'altro sul possibile, «diverso grado di curiosità del pubblico, che il delitto stimola più intensamente della lite». Più recentemente, a favore di una tendenziale prevalenza del principio di pubblicità vedasi F. Donati, *Trasparenza della giustizia e anonimizzazione dei provvedimenti giudiziari*, in A. Adinolfi - A. Simoncini (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, 2022, 609 ss.

[5] Fra i più recenti ed esaustivi contributi al rapporto tra informazione e oblio, v. P. De Martinis, *Oblio,* internet *e tutele. L'inibitoria*, Napoli, 2021, in particolare il Cap. III.

di quello penale, costituisce un principio essenziale dell'ordinamento democratico», posto a garanzia dell'imputato e del controllo della pubblica opinione sullo svolgimento del processo stesso; per tale ragione, le deroghe eventualmente concepite alla tutela della riservatezza dell'individuo dovranno necessariamente fondarsi su valutazioni attinenti alla sussistenza di gravi motivi, da ravvisare fra l'altro qualora i consociati possano risultare scossi «dall'allarme che suscita la commissione [di] alcuni tipi di reati che maggiormente colpiscono l'ordinata convivenza civile»[6]. Parallelamente ai parametri normativi così segnalati, un doveroso riferimento merita infine di essere riservato al Testo Unico dei doveri del giornalista, che al suo art. 3 (rubricato "Identità personale e diritto all'oblio") impone a quest'ultimo il rispetto del diritto all'identità personale, evitando di «far riferimento a particolari relativi al passato, salvo quando essi risultino essenziali per la completezza dell'informazione»[7].

2. La disciplina riservata al trattamento di dati contenuti in provvedimenti giurisdizionali. L'interpretazione dell'art. 52, d.lgs. 30 giugno 2003, n. 196 ad opera della giurisprudenza di legittimità e del Garante per la protezione dei dati personali

Il delicato tema della pubblicità dei provvedimenti giurisdizionali è attualmente regolato dagli artt. 51 e 52 del d.lgs. 30 giugno 2003, n. 196, collocati nell'ambito del suo Titolo III (riservato ai trattamenti in ambito giudiziario), Capo III (specificatamente riguardante l'informatica giuridica)[8].
L'art. 51, c. 1 dispone anzitutto che «[…] i dati identificativi delle questioni pendenti

[6] Corte cost., 27 luglio 1992, n. 373.

[7] Più nel dettaglio, l'art. 3 prosegue specificando come lo stesso professionista, nel diffondere a distanza di tempo dati identificativi del condannato, debba anche valutare «l'incidenza della pubblicazione sul percorso di reinserimento sociale dell'interessato e della sua famiglia, specialmente se congiunto (padre, madre, fratello) di persone di minore età». La valorizzazione di tale reinserimento stimola la raccomandazione, rivolta al giornalista, a non identificare il condannato solo con il reato commesso.

[8] Lo stesso Codice del 2003 prevedeva inoltre un trattamento specifico per i dati giudiziari agli artt. 21, 22 e 27, equiparati di fatto a quelli sensibili e individuati dall'art. 4, c. 1, lett. e) in tutti i dati idonei a rivelare il coinvolgimento di una persona in procedimenti di natura penale. Tali disposizioni, oggi abrogate, sono state sostituite dalle previsioni normative introdotte dal d.lgs. 101/2018, il quale, rimpiazzando la categoria dei dati giudiziari con quella dei "dati relativi a condanne penali e reati" (art. 2-*octies* del novellato Codice del 2003), richiama espressamente la disciplina di cui all'art. 10 GDPR: in base a quest'ultimo, «Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza […] deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica». Sul punto, si rimanda a M. Trapani, *Il trattamento dei dati relativi a condanne penali e reati e l'obbligo di designazione del Responsabile della protezione dei dati per i trattamenti effettuati dalle autorità giudiziarie*, in S. Scagliarini (a cura di), *Il "nuovo" codice in materia di protezione dei dati personali. La normativa italiana dopo il d.lgs. n. 101/2018*, Torino, 2019, 151 ss. Quanto agli artt. 51-52 del d.lgs. 30 giugno 2003, n. 196, una ricognizione generale di tali disposizioni è stata operata *ex multis* da R. De Nictolis, V. Poli, *Il diritto all'anonimato nel processo (art. 52 d.leg. 30 giugno 2003 n. 196)*, in *Giustizia Civile*, II, 2003, 495 ss.; G. Grasso, *Il trattamento dei dati di carattere personale e la riproduzione dei provvedimenti giudiziari*, in *Il Foro Italiano*, 5, 2018, 349 ss.

dinanzi all'autorità giudiziaria di ogni ordine e grado sono resi accessibili a chi vi abbia interesse anche mediante reti di comunicazione elettronica, ivi compreso il sito istituzionale della medesima autorità nella rete Internet»; il c. 2 aggiunge che «le sentenze e le altre decisioni dell'autorità giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete Internet, osservando le cautele previste dal presente capo». Tali cautele sono esplicitate dal successivo art. 52, parzialmente modificato per effetto del d.lgs. 10 agosto 2018, n. 101 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679). Posta la regola generale di cui al c. 7, relativa alla «diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali», la norma individua le ipotesi in cui tale principio incontra specifiche limitazioni: in osservanza del suo c. 1, infatti, «l'interessato può chiedere per motivi legittimi, con richiesta depositata nella cancelleria o segreteria dell'ufficio che procede prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria o segreteria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento». L'art. 52, c. 2, oltre a stabilire che sulla citata richiesta provvede in calce con decreto, senza ulteriori formalità, l'autorità che pronuncia la sentenza o adotta il provvedimento, attribuisce alla medesima autorità giudiziaria il potere di disporre d'ufficio che sia apposta l'annotazione di cui al c. 1, a tutela dei diritti o della dignità degli interessati; nell'estrinsecazione di tale potere officioso vengono in soccorso sia il disposto del c. 5 (il quale, oltre a richiamare l'art. 734-*bis* c.p. – e con ciò la diffusione delle generalità o dell'immagine delle vittime di reati a sfondo sessuale *ex* artt. 600-*bis* – 600-*quinquies* e 609-*bis* – 609-*octies* c.p. –, impone il divieto di condivisione delle generalità e di altri dati identificativi dai quali possa desumersi anche indirettamente l'identità di minori o delle parti coinvolte in procedimenti in materia di rapporti di famiglia e di stato delle persone), sia l'art. 9 del regolamento (UE) 2016/679, da cui si ricava la regola per cui sono soggetti a oscuramento obbligatorio i dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica e i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona[9].

Pertanto, rispetto ai limiti imposti dall'art. 51, c. 1 in relazione ai dati identificativi delle «questioni pendenti» (accessibili soltanto «a chi vi abbia interesse»), l'interazione con quelli contenuti in sentenze e altre decisioni di ogni ordine e grado depositate in cancelleria o segreteria è normalmente concessa a chiunque, salvo le suddette ipotesi di oscuramento obbligatorio o la sussistenza di un "motivo legittimo" tale da giusti-

[9] Come segnalato da F. Resta, *Pubblicità dei provvedimenti giurisdizionali e* privacy, in *Il trattamento dei dati personali in ambito giudiziario*, Quaderno 5, Scuola Superiore della Magistratura, 2021, 88, l'inclusione dei dati idonei a rivelare lo stato di salute e di quelli genetici e biometrici (art. 2-*septies* del Codice del 2003) tra i casi di oscuramento obbligatorio è stata raggiunta anche grazie all'interpretazione estensiva dell'art. 52 ad opera di Cass. civ., sez. I, 20 maggio 2016, n. 10510 (successivamente asseverata dal parere del Garante *privacy* n. 88 del 19 maggio 2020).

ficare una richiesta di soppressione degli stessi; come esplicitato dal c. 1, il soggetto legittimato alla richiesta è "l'interessato" (e non la sola parte processuale), ossia chiunque, a qualsiasi titolo, risulti identificabile in una sentenza o in altro provvedimento giurisdizionale[10].

Pare così evidente come l'ampiezza e l'effettività della tutela accordata alla privacy del soggetto coinvolto in un procedimento giudiziario dipenda anche e soprattutto dall'interpretazione che dottrina e giurisprudenza hanno a oggi offerto del concetto di "motivo legittimo"[11], chiaro riferimento ai «motivi preminenti e legittimi» cui l'art. 14, lett. a) della direttiva 95/46/CE (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) subordinava il diritto di opposizione della persona interessata al trattamento dei dati personali. Già in occasione dei primi commenti al Codice del 2003, la dottrina aveva osservato come la richiesta di anonimizzazione dei dati identificativi non sia necessariamente subordinata a ipotesi di trattamento illecito dei medesimi (potendo infatti essere domandata per motivi di pubblico interesse o nell'esercizio di una funzione pubblica), da cui la necessità di cogliere la "legittimità" dei motivi all'esito di un bilanciamento tra il diritto di informare ed essere informati con quello alla privacy[12]. Nel 2017, la Cassazione penale, recependo appieno le indicazioni nel frattempo offerte dal Garante privacy con provvedimento del 2 dicembre 2010[13], ha affermato come i motivi legittimi esatti dalla norma ben possano essere rappresentati dalla «delicatezza della vicenda oggetto di giudizio» o dalla «particolare natura dei dati contenuti nel provvedimento (ad esempio, dati sensibili[14])», ravvisando il connotato di "delicatezza" nella prospettiva di «negative conseguenze sui vari aspetti della vita sociale e di relazione dell'interessato (ad esempio, in ambito familiare o lavorativo), così andando ad incidere pesantemente sul diritto alla riservatezza del singolo» nell'ipotesi di diffusione dei dati a lui correlati[15]. La necessità di un'inter-

[10] Concordemente, L. A. Scarano, *Art. 52 (Dati identificativi degli interessati)*, in C. M. Bianca - F. D. Busnelli (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196*, Padova, 2007, Tomo I, 957. Ai sensi dell'art. 4 del regolamento (UE) 2016/679, «si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

[11] Per una suggestione sui rapporti fra la nozione di "motivi legittimi" (già adottata dall'art. 13 della l. 31 dicembre 1996, n. 675) e quella di "giusta causa" cara al Codice civile, v. G. Oppo, *Sul consenso dell'interessato*, in V. Cuffaro - V. Ricciuto - V. Zeno-Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, 125 ss.

[12] G. Bottino, *Articolo 7. Diritto di accesso ai dati personali ed altri diritti*, in *Codice della* privacy, cit., 83.

[13] *Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica*, Gazzetta Ufficiale n. 2 del 4 gennaio 2011. Il testo è disponibile all'indirizzo *garanteprivacy.it*.

[14] Originariamente individuati dall'art. 4, c. 1, lett. d) del d.lgs. 30 giugno 2003, n. 196 nei «dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale». Tale disposizione, oggi abrogata, è sostanzialmente confluita nell'art. 9 GDPR.

[15] In senso conforme, Cass. pen., sez. II, 25 giugno 2018, n. 29248 (occasione in cui le richieste di anonimizzazione proposte dai ricorrenti, relative all'opposizione a un sequestro preventivo, erano state respinte, «non essendo certamente idonei i riferimenti al danno alla reputazione suscettibile di

pretazione particolarmente rigorosa della locuzione recata dall'art. 52, insuscettibile di essere integrata dalla sola prospettazione di un danno reputazionale derivante dalla sottoposizione a procedimento penale, veniva esplicitata dagli stessi giudici con una riflessione di particolare pregnanza, osservandosi come «diversamente opinando, del resto, ogni processo penale dovrebbe comportare l'oscuramento dei dati personali, laddove, per un verso, si è qui in presenza di addebiti che scaturiscono da denunce formalizzate dai diretti interessati, come tali espressione della facoltà, propria dei cittadini di uno Stato di diritto ed a cui si attribuisce valore civico e sociale, di attivare in prima persona la risposta dell'ordinamento in casi di ritenuta violazione della legge penale, conseguentemente non riguardabili di per sé negativamente, salvo solo che esse celino fatti di simulazione di reato o di autocalunnia - nel caso, non ipotizzabili - ovvero ancora di calunnia, quest'ultima espressamente esclusa; per altro verso, l'esercizio di funzioni giurisdizionali non può in alcun modo risolversi nella gratuita attribuzione di una sorta di status superiore, tale da comportare una più intensa ed ampia tutela [= dell'imputato] rispetto a quella riconosciuta agli altri cittadini»[16].

La Suprema Corte ha affrontato il tema dell'anonimizzazione delle sentenze in tempi ancor più recenti ma in un numero di pronunce particolarmente contenuto, occasioni in cui l'assenza di considerazioni dirimenti ha palesato ancor più la necessità di un approccio inevitabilmente casistico nell'esegesi della formula in parola. A tal proposito, la Sezione V ha ritenuto di affermare come, in mancanza di una più puntuale indicazione da parte del legislatore, l'espressione "motivi legittimi" debba essere apprezzata «come sinonimo di "motivi opportuni"», da intendersi quale «meritevolezza delle ragioni addotte»; oltre a ciò, i togati si sono espressi nel senso che la richiesta di anonimizzazione sia da respingere «ogniqualvolta l'autorità giudiziaria ravvisi un equilibrato bilanciamento tra le esigenze di riservatezza del singolo e il principio della generale conoscibilità dei provvedimenti giurisdizionali e del contenuto integrale delle sentenze, quale strumento di democrazia e di informazione giuridica»[17].

3. Il tormentato tema del diritto all'oblio: aspetti definitori, disciplina e indirizzi giurisprudenziali

In ossequio alle premesse introduttive svolte in apertura, l'attenzione va ora focalizzata sul c.d. "diritto all'oblio"[18], il quale, al netto di una definizione sfuggevole e di una

essere arrecato alle società terze interessate ovvero a quella degli odierni indagati dalla pendenza del processo»); Cass. pen., sez. I, 24 dicembre 2021, n. 47126.

[16] Cass. pen., sez. VI, 13 marzo 2017, n. 11959. Così, egualmente, la poc'anzi citata Cass. pen., sez. II, 25 giugno 2018, n. 29248.

[17] Così Cass. civ., sez. V., 7 agosto 2020, n. 16807 (occasione in cui l'istanza di oscuramento era stata rigettata ritenendosi che la materia trattata – relativa ad atto di contestazione di sanzioni tributarie a seguito di rettifica del valore doganale delle merci trattate – non fosse né sensibile, né caratterizzata *in re ipsa* da particolare delicatezza); Cass. civ., sez. V, 10 agosto 2021, n. 22561. In particolare, l'ordinanza del 2020 si spinge ad affermare come «il concetto utilizzato dal legislatore [sia] per certo non felice».

[18] Fra le prime e più significative riflessioni organiche dedicate alla locuzione in esame, v. *ex multis* T. Auletta, *Diritto alla riservatezza e «droit à l'oubli»*, in G. Alpa - M. Bessone - M. Boneschi - L. Caiazza (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, 127 ss.; L. Crippa, *Il diritto all'oblio: alla ricerca*

giurisprudenza in costante evoluzione, costituisce essenzialmente un corollario del più ampio diritto alla riservatezza[19]. Quanto al suo fondamento costituzionale, alcuni autori lo collocano nell'alveo dell'art. 3, c. 1 Cost., stante il pensiero che la pari dignità sociale, fondamento per lo sviluppo della persona, passi anche attraverso la tutela dei propri dati personali[20]; in una prospettiva ancor più ampia, talaltri lo situano all'interno dell'art. 2 Cost., specificando tuttavia la sua propensione a entrare in conflitto con altri diritti quali quello di cronaca e, più ampiamente, quello alla libera manifestazione di pensiero di cui all'art. 21 Cost.[21].

Fra le innumerevoli riflessioni proposte circa l'individuazione dei suoi caratteri essenziali, il francese *droit à l'oubli* fu originariamente inquadrato come «diritto a farsi dimenticare»[22], per poi assumere progressivamente i tratti di un diritto connesso a specifici fatti od episodi del vissuto dell'individuo[23]. In Italia, la prima dottrina interessatasi al tema focalizzò l'attenzione sull'interesse «di un soggetto (le cui vicende furono un tempo note, perché ampiamente diffuse e pubblicizzate) a rientrare nell'anonimato dopo l'abbandono dell'attività da cui era derivata la notorietà e il conseguente giustificato interesse del pubblico»[24], mentre la giurisprudenza di legittimità operò un esplicito richiamo al diritto all'oblio soltanto con una decisione del 1998, laddove, di fronte alla pubblicazione di un articolo relativo all'incriminazione di un soggetto per gravi fatti di mafia - già vastamente reclamizzata dai rotocalchi negli anni precedenti

di un'autonoma definizione, in *Giustizia Civile*, 7-8, 1997, 1979 ss.; A. Masaracchia, *Sul c.d. "diritto all'oblio"*, in *Giurisprudenza costituzionale*, 1997, 3025 ss.; L. Rattin, *Il diritto all'oblio*, in *Archivio civile*, 2000, 1069 ss.; M. R. Morelli, voce *Oblio (diritto all')*, in *Enciclopedia del diritto*, Agg., VI, Milano, 2002, 848 ss.; S. Niger, *Il diritto all'oblio*, in G. Finocchiaro (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, Padova, 2007; M. Mezzanotte, *Il diritto all'oblio. Contributo allo studio della* privacy *storica*, Napoli, 2009. Per una breve riflessione sul diritto all'oblio quale contraltare dell'antica *damnatio memoriae*, S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, 2012, 404-407.

[19] Su tutti, G. Finocchiaro, *Diritto all'oblio e diritto di cronaca: una nuova luce su un problema antico*, in *Giustizia civile.com*, 15 gennaio 2019, la quale, richiamando la riflessione di G. B. Ferri, *Diritto all'informazione e diritto all'oblio*, in *Rivista di diritto civile*, 1990, 801 ss., parla di una situazione giuridica soggettiva che «"appartiene alle ragioni e 'alle regioni' del diritto alla riservatezza" e precede storicamente il diritto all'identità personale e il diritto alla protezione dei dati personali». Egualmente, G. Cassano, *Il diritto all'oblio esiste: è diritto alla riservatezza* (nota a Trib. Roma, 15 maggio 1995), in *Il diritto di famiglia e delle persone*, 1998, 76 ss. e, più recentemente, V. Bellomia, *Confini e tutele del diritto all'oblio digitale*, in M. Bianca (a cura di), *Memoria* versus *oblio*, Torino, 2019, 70 ss., par. 2; Id., *Diritto all'oblio e società dell'informazione*, Padova, 2020.

[20] Così T. E. Frosini, *Il diritto all'oblio e la libertà informatica*, in F. Pizzetti (a cura di), *Il caso del diritto all'oblio*, Torino, 2013, 94. Alla dignità dell'interessato fa peraltro riferimento l'art. 2 del Codice del 2003.

[21] E. Munarini, *Diritto all'oblio: significato, tutela e giurisprudenza recente*, in *Giuricivile*, 2018, 8

[22] Negli Stati Uniti, già T. M. Cooley, *A Treatise on the Law of Torts or the Wrongs which arise indipendent of Contracts*, Chicago, 1879, 29 ebbe a parlare di un *right to be let alone* (letteramente, "diritto a essere lasciati in pace"), capace di ricomprendere in sé la pretesa alla tranquillità mentale e spirituale. Per una riflessione sull'istituto nell'ambito del sistema dei *tort* e sulla sua rilevanza nell'epoca dei *mass media*, si rimanda a R. H. Adams Jr., *The Right to be Let Alone*, in *University of Florida Law Review*, vol. XVII, 1964-65, 597 ss.

[23] M. Morelli, voce *Oblio (diritto all')*, cit., 849. Circa l'originaria interpretazione del diritto all'oblio, l'Autore menziona la celebre vicenda giudiziaria riguardante il cantante Jean Ferrat, il quale, ritiratosi a vita privata con l'intenzione di far perdere le proprie tracce, era stato oggetto di un articolo contenente le sue vere generalità e altre informazioni connesse alla sua vita privata (numero di telefono, indirizzo della residenza e del domicilio, ecc...).

[24] G. B. Ferri, *Diritto all'informazione e diritto all'oblio*, cit., 807.

ma scollegata da riferimenti a una successiva sentenza di archiviazione nel frattempo intervenuta -, la Suprema Corte riconobbe un «legittimo interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore ed alla sua reputazione la reiterata pubblicazione di una notizia, in passato legittimamente divulgata»[25]. L'approccio al diritto all'oblio, originariamente modellato intorno al supporto della carta stampata ed evolutosi a fronte di problemi rimasti a tutt'oggi persistenti nel nostro sistema d'informazione (si pensi, a titolo d'esempio, agli effetti di una percepibile "asimmetria" comunicativa nell'ambito della cronaca giudiziaria, per cui gli sviluppi fattuali tali da scagionare un soggetto da determinate accuse tendono a non ricevere la medesima copertura mediatica invece riservata alle notizie che lo avevano posto in cattiva luce[26]), è inevitabilmente mutato con il progressivo sviluppo del mondo digitale, imponendo un confronto con problematiche quali quella di una maggiore facilità d'accesso alle informazioni disponibili in Rete e della piena accessibilità alle stesse per un periodo di tempo indeterminato. Nel 2012, occupandosi dell'archivio online di un noto quotidiano nazionale e della conservazione in esso di una notizia riguardante l'arresto per corruzione di un politico poi definitivamente assolto, i giudici di Piazza Cavour trattarono il diritto all'oblio quale strumento di salvaguardia della «proiezione sociale dell'identità personale, [del]l'esigenza del soggetto di essere tutelato dalla divulgazione di informazioni (potenzialmente) lesive in ragione della perdita (stante il lasso di tempo intercorso dall'accadimento del fatto che costituisce l'oggetto) di attualità delle stesse», giungendo a parlare di «verità della propria immagine nel momento storico attuale». Il suo riconoscimento impose così la contestualizzazione e l'aggiornamento della succitata notizia, anche se già collocata in un archivio storico, affinché questa potesse conservare i connotati di esattezza irrinunciabili tanto per la tutela dell'identità personale e morale dell'interessato, quanto del diritto del cittadino utente a ricevere un'informazione completa e corretta[27].

---

[25] Cass. civ., sez. III, 9 aprile 1998, n. 3679, in *Il Foro italiano*, 1998, I, c. 1834 ss., con nota di P. Laghezza, *Il diritto all'oblio esiste (e si vede)*. La sentenza è inoltre menzionata in S. Ruscica, P. Montone, *Il diritto all'oblio dopo il nuovo regolamento europeo sulla privacy*, in M. Maglio - M. Polini - N. Tilli (a cura di), *Manuale di diritto alla protezione dei dati personali*, Santarcangelo di Romagna, II ed., 2019, 184. Più recentemente, Cass. civ., sez. I, 19 maggio 2020, n. 9147 ha parlato di una pretesa a «non rimanere esposti, senza limiti di tempo, ad una rappresentazione non più attuale della propria persona, con pregiudizio alla reputazione ed alla riservatezza».

[26] Quanto al tema della spettacolarizzazione del processo penale a opera dei "circhi mediatici giudiziari", v. per tutti V. Manes, *La "vittima" del "processo mediatico": misure di carattere rimediale*, in *Diritto penale contemporaneo*, 3, 2017, 114 ss. La locuzione appena evocata impone un riferimento a D. S. Larivière, *Du cirque médiatico-judiciaire et des moyens d'en sortir*, Parigi, 1993. Più ampiamente, i contributi sul tema del giornalismo giudiziario, fenomeno che coinvolge la sociologia del diritto e, interdisciplinariamente, le norme deontologiche della categoria professionale di riferimento, si sprecano. Fra i primi e più rilevanti lavori, vedasi G. Giostra, *Giornalismo giudiziario: un ambiguo protagonista della giustizia penale*, in *Critica del diritto*, 1994, 54 ss. Circa il criterio della "essenzialità dell'informazione", locuzione adottata dall'art. 8 del Codice deontologico dei giornalisti quale condizione necessaria per la diffusione di notizie altrimenti lesive della dignità della persona, v. C. Malavenda - C. Melzi d'Eril - G. E. Vigevani, *Le regole dei giornalisti. Istruzioni per un mestiere pericoloso*, Bologna, 2012, 122-123. Occorre tener conto del fatto che tale carattere di "essenzialità", nella sua ineludibile indeterminatezza, può suggestionare il giornalista al punto da "asciugare" oltremodo la notizia, omettendo in tal senso dati e informazioni che effettivamente integrerebbero l'essenzialità medesima.

[27] Cass. civ., sez. III, 5 aprile 2012, n. 5525, in *Il Foro italiano*, 2013, 305 ss., con nota di E. Tucci; in *Danno e responsabilità*, 2012, 747 ss., con nota di M. Di Ciommo, R. Pardolesi, *Trattamento dei dati personali*

Un anno più tardi, la stessa Corte si trovò ad affrontare il caso di un quotidiano locale comasco responsabile di aver arbitrariamente collegato al ritrovamento di armi appartenenti alle Brigate Rosse un uomo residente nelle vicinanze, arrestato e condannato nel 1979 per condotte terroristiche; più nel dettaglio, i due articoli del 4 e 5 gennaio 1998 contenevano le sue generalità, una foto dell'epoca nonché un'intervista a sua detta mai rilasciata, facendo così riemergere un passato che l'interessato aveva cercato con grandi sforzi di far dimenticare. Nel riconoscere la fondatezza della pretesa attorea e condannare il direttore e l'editore del giornale al risarcimento del danno, la Cassazione affermava che «in tema di diffamazione a mezzo stampa, il diritto del soggetto a pretendere che proprie, passate vicende personali siano pubblicamente dimenticate […] trova limite nel diritto di cronaca solo quando sussista un interesse effettivo ed attuale alla loro diffusione, nel senso che quanto recentemente accaduto […] trovi diretto collegamento con quelle vicende stesse e ne rinnovi l'attualità. Diversamente, il pubblico e improprio collegamento tra le due informazioni si risolve in un'illecita lesione del diritto alla riservatezza, mancando la concreta proporzionalità tra la causa di giustificazione (il diritto di cronaca) e la lesione del diritto antagonista»[28].

Infine, in attesa di procedere all'esame delle più recenti decisioni elaborate dalla giurisprudenza nazionale e sovranazionale, meritevole di segnalazione è una sentenza del 2016, la quale, confermando la pronuncia di merito del Tribunale di Chieti-Ortona, aveva imposto la cancellazione dagli archivi di un giornale online di un articolo di cronaca relativo a un procedimento penale ancora in attesa di definizione (da cui il persistente interesse, almeno per la comunità locale, ad apprenderne gli sviluppi). A fondamento della propria decisione, la Cassazione poneva in risalto il fatto che la notizia originaria, oltre a essere facilmente reperibile e consultabile mediante il ricorso a motori di ricerca, fosse presente sul sito Web del quotidiano da più di due anni e mezzo, lasso temporale in cui, nonostante il perdurante svolgimento del processo,

e archivi storici accessibili in Internet: notizia vera, difetto di attualità, diritto all'oblio, in *Il Corriere Giuridico*, 2012, 747 ss., con nota di A. Di Majo, *Il tempo siamo noi*. Più nel dettaglio, la Cassazione aveva di fatto smentito la posizione assunta in merito dal Garante *privacy*, il quale, richiamando l'art. 4, c. 4, lett. a) del d.lgs. 196/2003, aveva ragionevolmente valorizzato le finalità di studio e di ricerca esaltate da tale norma, esprimendosi pertanto nel senso della conservazione dei contenuti contestati. Per una ricognizione attenta alle posizioni assunte in tema da parte del Garante, v. A. Mantelero, Right to be forgotten *ed archivi storici dei giornali. La Cassazione travisa il diritto all'oblio*, in *La nuova giurisprudenza civile commentata*, 2012, 843 ss. La pronuncia della Suprema Corte, riguardante nello specifico la gestione degli archivi informatici, si è esposta a ben vedere a plurime osservazioni critiche, in questa sede esclusivamente accennabili: fra di esse, le imponderabili difficoltà organizzative e i costi richiesti a ogni gestore di archivio per il quotidiano aggiornamento dello stesso (pena la certezza di rispondere in sede civile ed eventualmente penale qualora sia congiuntamente riscontrato un illecito trattamento dei dati dell'interessato), nonché il rilievo in base a cui un archivio, ponendosi quale obiettivo quello di organizzare dati appartenenti al passato, non possa che contenere informazioni e opinioni inevitabilmente superate, come facilmente comprensibile visionando la data di pubblicazione.

[28] Cass. civ., sez. III, 26 giugno 2013, n. 16111, in *Il Foro italiano*, 2013, c. 2442 ss.
Il complesso tema della conservazione di notizie riguardanti episodi di terrorismo ha incontrato inoltre l'interesse del Garante privacy, il quale, con provvedimento del 31 marzo 2016, ha negato il riconoscimento del diritto all'oblio nei confronti del responsabile di diversi reati aggravati di matrice terroristica commessi durante i c.d. "anni di piombo" (per i quali finì di scontare la relativa pena nel 2009), sostenendo che «nonostante il decorso del tempo dall'accadimento dei fatti, sussiste [comunque] il preponderante interesse pubblico al reperimento di notizie relative ad una delle pagine più buie della storia italiana». Il testo della decisione è disponibile all'indirizzo *gpdp.it*.

gli interessi pubblici sottesi al diritto di cronaca si sarebbero nel frattempo esauriti[29]. Comprensibilmente, una simile decisione suscita alcune perplessità, comunicando l'idea che, stante un'ineludibile componente di discrezionalità giudiziaria nel bilanciamento e nell'eventuale soccombenza del diritto d'informazione da parte dei lettori, il diritto di cronaca possa avere una scadenza così anticipata, anche e soprattutto quando un procedimento penale in corso giustificherebbe il persistente interesse degli utenti a conoscere la vicenda nella sua interezza.

Tra le fonti normative responsabili di una cristallizzazione del diritto all'oblio, il disposto dell'art. 13, l. 31 dicembre 1996, n. 675 confluì pochi anni più tardi in quello degli artt. 7 e 11 del Codice del 2003 (oggi abrogati), i quali operarono un primo, implicito riferimento a esso: mentre l'art. 7, c. 3, inerente al "diritto di accesso ai dati personali ed altri diritti", accordava all'interessato il diritto di ottenere l'aggiornamento e la rettificazione di dati personali che lo riguardavano nonché l'integrazione, la cancellazione, la trasformazione in forma anonima o il blocco di dati trattati in violazione di legge, l'art. 11, relativo alle modalità di trattamento dei dati, imponeva che questi ultimi fossero aggiornati e conservati in una forma che consentisse l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali erano stati raccolti o successivamente trattati.

Un anno dopo la presentazione presso la Camera dei Deputati della Dichiarazione dei diritti in Internet (che al tema dell'oblio dedica il suo art. 11)[30], l'entrata in vigore del regolamento (UE) 2016/679 (GDPR) ha fatto sì che la nozione di "diritto all'oblio" fosse espressamente recepita anzitutto dai "Considerando" 65 («Un interessato dovrebbe avere il diritto di ottenere la rettifica dei dati personali che lo riguardano e il «diritto all'oblio» se la conservazione di tali dati violi il presente regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento. In particolare, l'interessato dovrebbe avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia revocato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente regolamento [ ]»), 66 («Per rafforzare il «diritto all'oblio» nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali [ ]») e 156 («[ ] Gli Stati membri dovrebbero essere autorizzati a fornire, a specifiche condizioni e fatte salve adeguate garanzie per gli interessati, specifiche e deroghe relative ai requisiti in materia di informazione e ai diritti alla rettifica, alla cancellazione, all'oblio, alla limitazione del trattamento, alla portabilità dei dati personali, nonché al diritto di opporsi in caso di trattamento di dati personali per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica

[29] Cass. civ., sez. I, 24 giugno 2016, n. 13161, in *Il Foro italiano*, 2016, c. 2729 ss., con nota – condivisibilmente critica – di R. Pardolesi, *Diritto all'oblio, cronaca in libertà vigilata e memoria storica a rischio di soppressione*.

[30] Il testo è disponibile sul sito del Ministero dell'Interno all'indirizzo *interno.gov.it*.

o storica o per finalità statistiche [ ]»), incontrando poi la sua attuale disciplina all'art. 17, rubricato "Diritto alla cancellazione («diritto all'oblio»)": la norma in questione tutela ogni soggetto interessato riconoscendogli «il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo»; a quest'ultimo è conseguentemente imposto di intervenire qualora ricorra uno fra i motivi tassativamente indicati dalla stessa disposizione, tra cui la circostanza che i dati non siano più necessari rispetto alle finalità per le quali erano stati raccolti o altrimenti trattati, l'ipotesi in cui l'interessato revochi il consenso, i dati siano stati trattati illecitamente o i medesimi debbano essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento. Al contempo, il c. 3 opera un bilanciamento con altri diritti e interessi in gioco, affermando la soccombenza del diritto all'oblio qualora il trattamento sia necessario per l'espressione del diritto alla libertà d'espressione e d'informazione, per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, per motivi d'interesse pubblico nel settore della sanità pubblica, per fini d'archiviazione, nel pubblico interesse, di ricerca scientifica o storica o a fini statistici nonché per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria[31].

Stando a un'interpretazione letterale della previsione normativa appena richiamata, il diritto all'oblio si tradurrebbe pertanto nella sola facoltà di richiedere la cancellazione dei dati personali contestati[32]. Tuttavia, appare immediato rilevare come l'art. 17 sia in qualche modo completato dalla previsione normativa di cui all'art. 16, il quale, recependo in parte i contenuti dell'art. 7, c. 3 del Codice italiano del 2003, riconosce il diritto di rettifica (già richiamato dal summenzionato "Considerando" 65, che lo cita congiuntamente al diritto all'oblio): esso si traduce nel diritto per l'interessato a «ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa». In tal senso, la rettifica si presenta quale operazione dagli effetti meno drastici e decisamente più "malleabili" rispetto a quelli prodotti dalla cancellazione, assicurando all'interessato che i dati che lo riguardano siano corretti, aggiornati o integrati in relazione alle circostanze di fatto rilevate al momento della richiesta.

[31] Le limitazioni all'esercizio del diritto all'oblio previste dall'art. 17, par. 3, GDPR risultano ampliate in virtù delle ipotesi espressamente previste dagli artt. 2-*undecies* ("Limitazioni ai diritti dell'interessato") e 2-*duodecies* ("Limitazioni per ragioni di giustizia") del Codice del 2003: fra di esse, la prospettiva di un pregiudizio effettivo e concreto agli interessi tutelati in base alle disposizioni in materia di riciclaggio e a quelle in materia di sostegno alle vittime di richieste estorsive, nonché all'attività di Commissioni parlamentari d'inchiesta, allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria e alla riservatezza dell'identità del dipendente che segnali l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio ai sensi della l. 30 novembre 2017, n. 179 (c.d. *whistleblowing*). Sul punto, v. B. Meo, *Articolo 17 - Diritto alla cancellazione*, in G. M. Riccio - G. Scorza - E. Belisario (a cura di), *GDPR e Normativa Privacy. Commentario*, Milano, II ed., 2022, 234-235.

[32] In tal senso, si consideri la riflessione operata da V. Cuffaro, *Cancellare i dati personali: dalla* damnatio memoriae *al diritto all'oblio*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, 219 ss., il quale focalizza l'attenzione sulla «mancanza di autonomia» del diritto all'oblio «rispetto alla radicale pretesa alla cancellazione dei dati».

3.1. Il diritto alla deindicizzazione nella giurisprudenza della Corte di Giustizia dell'Unione Europea

Un'esaustiva ricognizione intorno all'essenza del diritto all'oblio non può prescindere da un richiamo al celebre caso *Google Spain*[33], inerente più nello specifico al tema della deindicizzazione (*delisting*) e così alla giurisprudenza della Corte di Giustizia dell'Unione Europea precedente all'introduzione del GDPR. Vale in questa sede premettere come la deindicizzazione stessa, lungi dal comportare una radicale rimozione di un contenuto dal Web, miri piuttosto a impedire – o, comunque, a limitare considerevolmente le probabilità – che quest'ultimo possa essere reperito attraverso l'impiego di motori di ricerca[34]; in concreto, ciò si realizza mediante la rimozione dell'informazione interessata dalle SERP (*Search Engine Results Pages*) del motore stesso, consentendone conseguentemente la reperibilità soltanto a chi conosca l'indirizzo URL della pagina di provenienza[35]. In tal senso, come osservato qualche anno più tardi dalla Cassazione italiana, la richiesta di deindicizzazione si presenta quale «soluzione di ragionevole compromesso» rispetto alla più netta cancellazione ai fini di un efficace «bilanciamento tra i diritti del singolo e quelli della collettività», mirando al c.d. ridimensionamento della visibilità mediatica e con ciò rientrando a pieno titolo nell'alveo del più ampio diritto all'oblio[36].

Nel caso evocato, Mario Costeja González, avvocato spagnolo, aveva presentato all'*Agencia Española de Protección de Datos* un reclamo contro l'editore del quotidiano *La Vanguardia* nonché contro Google Spain e Google Inc., chiedendo all'editore che un articolo relativo a una sua passata vicenda giudiziaria recante alcuni dati personali fosse modificato o rimosso e al colosso informatico che questi ultimi non figurassero

[33] Il riferimento è a CGUE, Grande Sezione, C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, (2014), disponibile all'indirizzo *eur-lex.europa.eu*. Tale pronuncia, la quale ha incontrato fin da subito l'interesse della dottrina, è stata oggetto in Italia di numerosissimi contributi, fra cui meritano di essere segnalati quelli di M. Di Ciommo, *Quello che il diritto non dice. Internet e oblio*, in *Danno e responsabilità*, 12, 2014, 1101 ss.; G. Resta - V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google-Spain*, Roma, 2015; M. Partipilo, *L'oblio della notizia. Tra nuove leggi e ultime sentenze quale destino per il diritto di cronaca?*, Roma, 2020, 55 ss.

[34] F. Pizzetti, *Le Autorità garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain: è tempo di far cadere il 'Velo di Maya'*, in G. Resta, V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google-Spain*, cit., 258, parla del diritto alla deindicizzazione come di un «diritto a non essere facilmente trovato», richiamando in tal senso l'espressione «right not to be found easily» (in luogo di un pressoché utopico «right to be forgotten») impiegata da A. Palmieri - R. Pardolesi, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, in *Nuovi quaderni del Foro italiano*, 1, 2014.
Per una trattazione del diritto alla deindicizzazione quale "anima" giurisprudenziale del diritto all'oblio di "impronta eurounitaria", si rimanda a R. Pardolesi, *L'ombra del tempo e (il diritto al)l'oblio*, in *Questione giustizia*, 1, 2017, disponibile all'indirizzo *questionegiustizia.it*. Quanto a una lettura del diritto alla deindicizzazione quale "new wave" rispetto al diritto all'oblio tradizionalmente inteso, v. S. Bonavita, *Le ragioni dell'oblio*, in *Ciberspazio e Diritto*, 1, 2017, 85 ss.

[35] In realtà, oltre a rimanere presenti sui siti d'origine e nelle copie *cache*, i contenuti deindicizzati da Google continuano a essere reperibili all'indirizzo Internet: http://hiddenfromgoogle.com, piattaforma che rende «accessibili proprio quelle informazioni a cui i *webmaster* avevano riservato, nelle intenzioni, un minor grado di conoscibilità»: così C. Comella, *Indici, sommari, ricerche e aspetti tecnici della 'de-indicizzazione'*, in *Il diritto all'oblio su Internet dopo la sentenza Google-Spain*, cit., 190.

[36] Così Cass. civ., sez. I, 27 marzo 2020, n. 7559.

più fra i risultati di ricerca; alla base di tale richiesta vi era il rilievo circa la vetustà della notizia riportata, reputato che la stessa dovesse ormai considerarsi priva di qualsivoglia rilevanza mediatica. La suddetta *Agencia*, respinto il reclamo diretto contro l'editore (il quale, ad avviso dell'autorità, avrebbe legittimamente divulgato la notizia esaminata), aveva invece accolto quello riguardante Google Spain e Google Inc., chiedendo pertanto alle due società di compiere tutte le operazioni necessarie affinché i dati interessati fossero rimossi dai loro indici. A seguito di due ricorsi promossi da Google, l'*Audiencia Nacional*, recettrice degli stessi, aveva invocato l'intervento della Corte di Giustizia con apposita domanda di pronuncia pregiudiziale *ex* art. 267 TFUE. La Grande Sezione, richiamando l'allora vigente direttiva 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione dei medesimi, aveva evidenziato come quest'ultima riconoscesse nei gestori dei motori di ricerca i responsabili del relativo trattamento di dati personali[37], da cui l'insorgere di obblighi quali la rimozione dei dati inadeguati, non pertinenti o non più pertinenti rispetto alle finalità per cui erano stati raccolti e diffusi sul Web. Tale statuizione consente di comprendere la netta distinzione tra la figura del gestore del motore di ricerca e quella del responsabile del sito ove i dati siano stati originariamente pubblicati, così come quella fra la richiesta di deindicizzazione (da rivolgere al primo, il quale raccoglie, estrae, registra e organizza i dati nell'ambito dei suoi programmi di indicizzazione) e la richiesta di cancellazione, da inoltrare invece al soggetto terzo che abbia provveduto a caricare e diffondere i dati online: la sentenza, infatti, specifica come l'obbligo gravante sul gestore del motore di ricerca di «sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona» debba essere rispettato «anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita»[38]. Quanto alla necessità di definire l'ambito di applicazione territoriale della direttiva - stante il coinvolgimento di una società avente la sua sede legale negli Stati Uniti -, la Corte riconosceva in Google Spain una "filiale" di Google Inc. destinata alla promozione e alla vendita agli abitanti di uno Stato membro degli spazi pubblicitari proposti dal motore di ricerca, da cui la sua riconducibilità alla nozione di "stabilimento" accolta dalla direttiva (art. 4, par. 1, lett. a) e la piena operatività di quest'ultima nel caso di specie; a tal proposito, i giudici avevano ritenuto irrilevante l'argomento addotto da Google Inc., fondato sul rilievo in base a cui il trattamento dei dati personali ad opera

[37] CGUE, Grande Sezione, C-131/12, cit., § 100: «L'articolo 2, lettere b) e d), della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, deve essere interpretato nel senso che, da un lato, l'attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come «trattamento di dati personali», ai sensi del citato articolo 2, lettera b), qualora tali informazioni contengano dati personali, e che, dall'altro lato, il gestore di detto motore di ricerca deve essere considerato come il «responsabile» del trattamento summenzionato, ai sensi dell'articolo 2, lettera d), di cui sopra».

[38] *Ibid.*

di Google Search non sarebbe stato concretamente condotto nel contesto delle attività svolte nello stabilimento iberico. La pronuncia veniva chiusa da alcune considerazioni inerenti ai presupposti per l'accoglimento di una richiesta di deindicizzazione formulata in ossequio agli artt. 12 e 14 della direttiva, segnalandosi la necessità di operare un riferimento agli artt. 7 e 8 CEDU nel bilanciamento fra il diritto alla deindicizzazione invocato dal cittadino europeo e quello del grande pubblico a recepire le informazioni veicolate dalla notizia[39]. La Corte risolveva tale conflitto affermando una tendenziale prevalenza dei diritti fondamentali affermati dalla Convenzione tanto «sull'interesse economico del gestore del motore di ricerca», quanto su quello del medesimo pubblico «ad accedere all'informazione suddetta in occasione di un ricerca concernente il nome di questa persona»; tuttavia, ogniqualvolta dovessero sussistere «ragioni particolari» quali il particolare «ruolo ricoperto da tale persona nella vita pubblica, [ ] l'ingerenza nei suoi diritti fondamentali» sarebbe in questo caso «giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso [ ] all'informazione»[40].

In questi termini, l'unico limite all'esercizio del diritto a ottenere la deindicizzazione veniva individuato dai giudici lussemburghesi nel particolare interesse pubblico all'apprendimento della notizia contestata, circostanza ricorrente nella prassi in ragione della notorietà e/o del ruolo pubblico rivestito dal soggetto cui le informazioni sono riferite[41]. Ciò nonostante, la sentenza esaminata non si premurava di enunciare criteri e parametri valutativi volti a uniformare le procedure di rimozione di tali dati, lasciando così al gestore del motore di ricerca - un soggetto privato privo delle competenze e della sensibilità necessarie per la valutazione delle singole vicende vagliate – un vero e

[39] Con specifico riferimento alle potenziali lesioni al diritto al rispetto della vita privata e familiare sancito dall'art. 8 CEDU, si considerino le riflessioni svolte ivi, § 80: «[...] un trattamento di dati personali, quale quello in esame nel procedimento principale, effettuato dal gestore di un motore di ricerca, può incidere significativamente sui diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, nel caso in cui la ricerca con l'aiuto di tale motore venga effettuata a partire dal nome di una persona fisica, dal momento che detto trattamento consente a qualsiasi utente di Internet di ottenere, mediante l'elenco di risultati, una visione complessiva strutturata delle informazioni relative a questa persona reperibili su Internet, che toccano potenzialmente una moltitudine di aspetti della sua vita privata e che, senza il suddetto motore di ricerca, non avrebbero potuto – o solo difficilmente avrebbero potuto – essere connesse tra loro, e consente dunque di stabilire un profilo più o meno dettagliato di tale persona. Inoltre, l'effetto dell'ingerenza nei suddetti diritti della persona interessata risulta moltiplicato in ragione del ruolo importante che svolgono Internet e i motori di ricerca nella società moderna, i quali conferiscono alle informazioni contenute in un siffatto elenco di risultati carattere ubiquitario». Sul rilievo assunto della Convenzione Europea dei Diritti dell'Uomo nella pronuncia della CGUE, v. O. Pollicino, *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel* reasoning *di* Google Spain, in *Il diritto dell'informazione e dell'informatica*, 4-5, 2014, 569 ss.

[40] Ivi, § 99.

[41] Una prima applicazione giurisprudenziale di tali principi si è avuta in Italia grazie a una sentenza del Tribunale di Roma, sez. I civ., 3 dicembre 2015, n. 23771, la quale ravvisava nel fattore temporale e nel ruolo svolto dal ricorrente nella vita pubblica i due essenziali elementi costitutivi del diritto alla deindicizzazione. La pronuncia è stata oggetto di un primo commento da parte di F. Russo, *Diritto all'oblio e motori di ricerca: la prima pronuncia dei Tribunali italiani dopo il caso* Google Spain, in *Danno e responsabilità*, 3, 2016, 299 ss.
In seno alla letteratura penalistica, per un'analitica ricognizione del diritto alla riservatezza e delle sue possibili declinazioni anche in rapporto all'interesse pubblico alla divulgazione di una notizia vedasi già F. Bricola, *Prospettive e limiti della tutela penale della riservatezza*, in *Rivista italiana di diritto e procedura penale*, 1967, in particolare 1083 ss.

proprio arbitrio nel vaglio di fondatezza dell'istanza di deindicizzazione[42].

Per quanto attiene all'estensione geografica dell'azione richiesta al gestore di un motore di ricerca, profilo rispetto cui la decisione sul caso *Google Spain* non aveva offerto indicazioni, alcune "Linee guida sull'esercizio del diritto all'oblio" elaborate pochi mesi dopo dal Gruppo dei Garanti europei si erano premurate di suggerire che il procedimento di deindicizzazione, lungi dal limitarsi ai soli domini europei, dovesse al contrario ricomprendere ogni altro dominio rilevante, ivi compreso quello ".com"[43]. Tuttavia, tale presa di posizione era destinata a essere smentita da una successiva pronuncia del medesimo organo giurisdizionale.

A cinque anni dal caso *Google Spain*, con un'importante decisione resa in data 24 settembre 2019 dalla stessa Grande Sezione nella causa C-507/17[44] (anche nota come "sentenza Google 2"), la Corte di Giustizia è intervenuta a seguito della sanzione di € 100.000 inflitta dalla *Commission nationale de l'informatique et des libertés* a Google LLC (succeduta alla Google Inc.), la quale, nell'accogliere una richiesta di deindicizzazione, aveva provveduto a eliminare i link dei soli risultati visualizzabili nello Stato in cui era stata compiuta la ricerca mediante tale browser: il colosso di Mountain View, infatti, si era rifiutato di applicare la deindicizzazione a tutte le estensioni del nome di dominio del suo motore di ricerca. Chiamati a pronunciarsi sulla portata territoriale del diritto in questione, i giudici europei hanno osservato come «allo stato attuale, non sussista, per il gestore di un motore di ricerca che accoglie una richiesta di deindicizzazione presentata dall'interessato, eventualmente, a seguito di un'ingiunzione di un'autorità di controllo o di un'autorità giudiziaria di uno Stato membro, un obbligo, derivante dal diritto dell'Unione, di effettuare tale deindicizzazione su tutte le versioni del suo motore»[45]. Pur affermandosi come l'ampia tutela garantita all'individuo dal diritto all'oblio dovrebbe comportare una cancellazione delle informazioni contestate su tutte le estensioni del nome di dominio del motore di ricerca, la Corte considera però come tale diritto debba necessariamente essere sottoposto a bilanciamento in ordinamenti di Stati terzi rispetto all'Unione Europea che accordano alla protezione dei dati personali una rilevanza minore rispetto al diritto all'informazione degli utenti (nonché a libertà quali quella d'espressione e d'impresa) o, addirittura, non riconoscono del tutto il diritto alla deindicizzazione[46]. Circoscritta così l'estensione del diritto ai confini dell'Unione europea, si è constatato come né la direttiva 95/46/CE, né il regolamento (UE) 2016/679 nel frattempo introdotto (e, in particolare, il suo art. 17) attribuiscano espressamente

[42] Al netto della possibilità di impugnare l'eventuale rigetto in sede giurisdizionale, circa l'assenza di una «chiara procedura di rimozione» si era espresso A. Mantelero, *Il futuro regolamento Ue sui dati personali e la valenza 'politica' del caso Google: ricordare e dimenticare nella digital economy*, in *Il diritto all'oblio su Internet dopo la sentenza Google-Spain*, cit., 137.

[43] Il riferimento è alle *Guidelines on the implementation of the court of justice of the european union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEDP) and Mario Costeja González C-131/12* del 26 novembre 2014, disponibili all'indirizzo *ec.europa.eu*. Sul punto, B. Meo, cit., 240; M. Partipilo, cit., 60.

[44] CGUE, Grande Sezione, C-507/17, *Commission nationale de l'informatique et des libertés (CNIL) c. Google LLC*, (2019). Il testo della sentenza è disponibile all'indirizzo *curia.europa.eu*.

[45] Ivi, § 64.

[46] Ivi, §§ 13. 4, 59 e 60.

al diritto medesimo una portata tale da coinvolgere territori extra-comunitari; al contempo, lo stesso diritto dell'Unione non ha mai previsto «strumenti e meccanismi di cooperazione [ ] per quanto riguarda [ ] una deindicizzazione al di fuori dell'Unione»[47]. La pronuncia, pur giustificata da un'interpretazione letterale delle disposizioni richiamate e dalla natura vincolante delle stesse per i soli Stati membri, si espone ad alcuni rilievi critici. In primo luogo, è possibile osservare come l'effettività di un diritto consistente nella pretesa a che determinate informazioni incontrino la minor risonanza mediatica possibile, subordinata a un controllo esteso all'intero Web, risulti inevitabilmente compressa a fronte della perimetrazione esclusivamente europea degli obblighi del gestore. In seconda istanza, scandagliando attentamente la decisione appena considerata, non va tralasciato un importante *obiter dictum*, riconoscendosi «che il diritto dell'Unione, pur se [ ] non impone, allo stato attuale, che la deindicizzazione accolta verta su tutte le versioni del motore di ricerca in questione, neppure lo vieta. Pertanto, un'autorità di controllo o un'autorità giudiziaria di uno Stato membro resta competente ad effettuare, conformemente agli standard nazionali di protezione dei diritti fondamentali […], un 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 e, al termine di tale bilanciamento, richiedere, se del caso, al gestore di tale motore di ricerca di effettuare una deindicizzazione su tutte le versioni di suddetto motore»[48]. Chiaramente, l'assenza di un obbligo positivo lascia prevedere che una richiesta di deindicizzazione estesa a ogni dominio, pur astrattamente formulabile, risulterà evasa in base all'insindacabile discrezionalità del gestore medesimo.

Per concludere la rassegna inerente alla giurisprudenza della Corte di Giustizia, meritevole di menzione è pure una sentenza resa contestualmente a quella appena esaminata nella causa C-136/17[49], laddove i ricorrenti avevano domandato la deindicizzazione di alcuni articoli di cronaca giudiziaria recanti informazioni circa lo stato di un procedimento penale istruito nei loro confronti, il cui scenario era mutato al passaggio verso una successiva fase processuale. I giudici, riconoscendo il diritto alla deindicizzazione nell'ipotesi in cui le informazioni controverse si riferiscano a una fase precedente di un procedimento giudiziario non più corrispondente alla situazione vigente al momento della richiesta, hanno ritenuto che tale valutazione imponga al gestore di tener conto «di tutte le circostanze del caso di specie, quali, in particolare, la natura e la gravità dell'infrazione di cui trattasi, lo svolgimento e l'esito di tale procedura, il tempo trascorso, il ruolo rivestito da tale persona nella vita pubblica e il suo comportamento in passato, l'interesse del pubblico al momento della richiesta, il contenuto e la forma della pubblicazione nonché le ripercussioni della pubblicazione per tale persona»[50]. Operando una precisazione non priva di rilievo, la Corte

[47] Ivi, §. 63.

[48] CGUE, Grande Sezione, C-507/17, cit., § 72.

[49] CGUE, Grande Sezione, C-136/17, *GC, AF, BH, ED c. Commission nationale de l'informatique et des libertés (CNIL)*, (2019). Il testo è disponibile all'indirizzo *curia.europa.eu*.

[50] Ivi, § 77. Circa la non invocabilità del diritto all'oblio in relazione a vicende giudiziarie di particolare gravità e il cui *iter* processuale risulti concluso da poco tempo, vedasi *ex multis* il provvedimento del Garante *privacy* del 6 ottobre 2016, n. 5690378, relativo al patteggiamento richiesto da un ex consigliere comunale imputato per condotte di corruzione e truffa. Il testo del provvedimento è disponibile all'indirizzo *garanteprivacy.it*.

ha aggiunto come, anche nel caso in cui non ricorrano gli estremi per l'accoglimento di una simile richiesta, il gestore debba comunque provvedere «a sistemare l'elenco dei risultati in modo tale che l'immagine globale che ne risulta per l'utente di Internet rifletta la situazione giudiziaria attuale, il che necessita, in particolare, che compaiano per primi, nel suddetto elenco, i link verso pagine web contenenti informazioni a tal proposito»[51].

3.2. Le più recenti elaborazioni nazionali e sovranazionali in tema di diritto all'oblio

Il diritto all'oblio, espressamente menzionato dal citato art. 17 GDPR e filtrato attraverso le pronunce della Corte di Giustizia dell'Unione Europea[52], risulta ad oggi sprovvisto in Italia di una sua espressa definizione e disciplina, da cui l'irrinunciabile, costante ricorso all'attività esegetica della giurisprudenza di legittimità nel tentativo di comprenderne il perimetro e l'ambito di operatività.

Nel 2018, la Cassazione aveva annullato con rinvio una sentenza della Corte di Appello di Roma la quale, rigettando la domanda di risarcimento del danno presentata da un famoso cantante della capitale, aveva riconosciuto la liceità della trasmissione di alcune immagini televisive riprese nel 2000 e riproposte cinque anni dopo senza il consenso dell'artista: a tal proposito, i giudici avevano ravvisato nella notorietà del personaggio e nell'interesse pubblico alla diffusione di tali contenuti una deroga alla necessità del consenso medesimo, giudicando peraltro sussistente l'esimente del diritto di satira (essendo il video corredato da alcuni commenti sarcastici in risposta al rifiuto del cantante a prestarsi a un'intervista) e, contestualmente, l'inesistenza del preteso diritto all'oblio. Ribaltando la decisione, la Suprema Corte rifiutava l'idea che la mera notorietà del ricorrente potesse da sola escludere la sussistenza del diritto invocato, ritenendo piuttosto che «il diritto fondamentale all'oblio può subire una compressione, a favore dell'ugualmente fondamentale diritto di cronaca, solo in presenza di specifici e determinati presupposti: 1) il contributo arrecato dalla diffusione dell'immagine o della notizia ad un dibattito di interesse pubblico; 2) l'interesse effettivo ed attuale alla diffusione dell'immagine o della notizia (per ragioni di giustizia, di polizia o di tutela dei diritti e delle libertà altrui, ovvero per scopi scientifici, didattici o culturali), da reputarsi mancante in caso di prevalenza di un interesse divulgativo o, peggio, meramente economico o commerciale del soggetto che diffonde la notizia o l'immagine; 3) l'elevato grado di notorietà del soggetto rappresentato, per la peculiare posizione rivestita nella vita pubblica e, segnatamente, nella realtà economica o politica del paese; 4) le modalità impiegate per ottenere e nel dare l'informazione, che deve essere veritiera (poiché attinta da fonti affidabili e con un diligente lavoro di ricerca), diffusa con modalità non

[51] Ivi, § 78.

[52] Un ulteriore, importante strumento esegetico è a tutt'oggi rappresentato dalle *Linee Guida 5/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca* redatte dal Comitato europeo per la protezione dei dati personali (EDBP), disponibili nella loro versione 2.0 (7 luglio 2020) all'indirizzo *edpb.europa.eu*.

eccedenti lo scopo informativo, nell'interesse del pubblico, e scevra da insinuazioni o considerazioni personali, sì da evidenziare un esclusivo interesse oggettivo alla nuova diffusione; 5) la preventiva informazione circa la pubblicazione o trasmissione della notizia o dell'immagine a distanza di tempo, in modo da consentire all'interessato il diritto di replica prima della sua divulgazione al grande pubblico»[53]. In questi termini, la Cassazione è ricorsa a una tecnica decisoria simile a quella adottata in occasione della celebre "sentenza decalogo" che per prima enunciò i tre fondamentali requisiti del diritto di cronaca[54], pur destando alcuni dubbi quanto all'interpretazione e al rispetto dei parametri enucleati: mentre il concetto di "notorietà" *sub* 3) risulta svincolato da riferimenti temporali (portando a domandarsi se essa sia tale da prevalere sul diritto all'oblio qualora sussistente al momento dei fatti narrati o a quello del procedimento giudiziario in corso di svolgimento), la condizione *sub* 5) si rivela all'atto pratico pressoché irrealizzabile, soprattutto nei casi in cui, diversamente da quanto avviene per la pubblicazione di rubriche e iniziative editoriali programmate con largo anticipo, i tempi ristretti dell'attività giornalistica non consentano di attendere la replica del soggetto interessato[55].

La stessa Corte tornava a esprimersi su tali parametri soltanto un anno dopo. I giudici romani della Sezione III[56] erano chiamati a pronunciarsi circa la rievocazione, a opera di un quotidiano sardo, di un violento uxoricidio avvenuto ventisette anni prima – condotta per la quale il responsabile aveva scontato una lunga pena detentiva –, giustificata a detta del giornale e dell'autore dell'articolo dalla sua comparizione nel contesto di una rubrica destinata a episodi di cronaca nera avvenuti nel cagliaritano negli ultimi decenni (da cui l'asserito pubblico interesse alla sua "riemersione"). Stanti i dubbi quanto al necessario, contestuale rispetto di tutti i summenzionati requisiti nonché l'intervento del più volte evocato art. 17 GDPR specificatamente riservato al diritto all'oblio, i togati optavano per un'ordinanza di remissione alle Sezioni Unite, pronunciatesi infine con sentenza del 22 luglio 2019[57]. Operati alcuni cenni al quadro normativo interno ed

[53] Cass. civ., sez. I, 20 marzo 2018, n. 6919, in *Il Foro italiano*, 2018, c. 1145 ss., con nota di R. Pardolesi - S. Bonavita, *Diritto all'oblio e buio a mezzogiorno*; in *Diritto e giustizia*, 2018, 2 ss., con nota di D. Bianchi, *Oblio batte satira quando il personaggio noto non è figura pubblica.*

[54] Il riferimento è a Cass. civ., sez. I, 18 ottobre 1984, n. 5259.
La sussistenza del requisito della continenza di espressione, congiuntamente alla rilevanza pubblica attuale della notizia, era stata posta dalla Cassazione a fondamento di una pronuncia di segno opposto (Cass. pen., sez. V, 3 agosto 2017, n. 38747). In quell'occasione, la Suprema Corte aveva rigettato il ricorso presentato da Vittorio Emanuele di Savoia, il quale aveva denunciato il direttore e il cronista de *la Repubblica* per la pubblicazione, in occasione di una visita dello stesso nobile italiano alla Reggia di Venaria nel corso della cerimonia di riapertura, di un articolo evocativo del celebre episodio del turista tedesco ucciso mentre dormiva nei pressi della sua imbarcazione, occorso nel lontano 1978. Il diritto della collettività a essere informata e aggiornata su fatti da cui dipende la formazione dei suoi convincimenti veniva in questo caso ritenuto prevalente rispetto a quello all'oblio, posta la liceità dell'articolo contestato (il quale, lungi dall'operare nuove insinuazioni, si limitava a riportare un fatto «pacifico nella sua materialità») e parimenti quella della critica a ritenere inopportuna la presenza dell'esponente di casa Savoia alla manifestazione piemontese. La sentenza è stata annotata da R. Pardolesi, *«Il mio regno per un('isola di) Cavallo»: limiti del diritto all'oblio di un aspirante erede al trono*, in *Il Foro italiano*, 2017, II, c. 649 ss.

[55] M. Partipilo, cit., 101-102.

[56] Cass. civ., sez. III, ord. 5 novembre 2018, n. 28084.

[57] Cass. civ., SS. UU., 22 luglio 2019, n. 19681, in *Il Foro italiano*, 2019, c. 3071 ss., con nota di R. Pardolesi, *Oblio e anonimato storiografico: «usque tandem...»?*; in *Il Corriere Giuridico*, 2019, 1195 ss., con nota di

europeo nonché alla giurisprudenza della Corte sull'argomento, le Sezioni Unite sovvertivano il giudizio reso dalla Corte di Appello di Cagliari (che aveva ritenuto prevalente il diritto di cronaca), riconoscendo il diritto all'oblio dell'interessato; nello specifico, il bilanciamento fra i due diritti veniva raggiunto affermando che «la menzione degli elementi identificativi delle persone che di quei fatti e di quelle vicende furono protagoniste» è lecita solo nell'ipotesi in cui si riferisca a personaggi che destino nel momento presente l'interesse della collettività, sia per ragioni di notorietà che per il ruolo pubblico rivestiti; viceversa, «prevale il diritto degli interessati alla riservatezza rispetto ad avvenimenti del passato che li feriscano nella dignità e nell'onore e dei quali si sia ormai spenta la memoria collettiva». La Corte coglieva così l'occasione per distinguere fra diritto di cronaca e «diritto alla rievocazione storica (storiografica)» di un fatto, il quale, in assenza di «elementi nuovi tali per cui la notizia ritorni di attualità, di modo che diffonderla nel momento presente rappresenti ancora una manifestazione del diritto di cronaca [ ] non può godere della stessa garanzia costituzionale che è prevista per il diritto di cronaca». Quanto alle ricadute pratiche, la Suprema Corte osservava, con un'affermazione perentoria, come la storiografia giornalistica che non riguardi un personaggio pubblico o «fatti che per il loro stesso concreto svolgersi implichino il richiamo ai nomi dei protagonisti» dovrebbe «svolgersi in forma anonima, perché nessuna particolare utilità può trarre chi fruisce di quell'informazione dalla circostanza che siano individuati in modo preciso coloro i quali tali atti hanno compiuto»[58]. Non è arduo comprendere come la decisione appena considerata si sia esposta a una ferma e compatta reazione da parte della dottrina, tanto per l'approccio eccessivamente radicale alle problematiche emerse (mancando all'atto pratico un criterio univoco e/o una soglia temporale per l'individuazione di un confine fra "storia" e "attualità"[59]) quanto per l'impossibilità di predeterminare i dati che una ricognizione storica realmente in grado di fornire al lettore una conoscenza completa dei fatti narrati dovrebbe mantenere o espungere. A voler abbracciare una posizione radicale, infatti, il grande pubblico vanterebbe tendenzialmente una mera curiosità - e non già un vero e proprio interesse meritevole di tutela - alla conoscenza delle generalità dell'autore di una condotta delittuosa (da cui la riduzione di quei "fatti che per il loro stesso concreto svolgersi implichino il richiamo ai nomi dei protagonisti" a mera ipotesi residuale), dati anagrafici che invece, in presenza di quel reo particolarmente celebre cui la Corte allude in termini derogatori, finirebbero *sine die* alla mercé degli utenti.

Un conclusivo richiamo alla giurisprudenza della Corte Europea dei Diritti dell'Uomo impone il riferimento ad almeno due pronunce rese dai giudici di Strasburgo. Nel 2017, la Corte si esprimeva riguardo il ricorso presentato da Boris Fuchsmann, imprenditore ucraino con cittadinanza tedesca, sulla base dell'art. 8 CEDU, giustificato dal mancato oscuramento da parte della Corte di Appello di Düsseldorf di un articolo comparso

V. Cuffaro, *Una decisione assennata sul diritto all'oblio*; in questa rivista, 3, 2019, 203 ss., con nota di S. Peron, *Il difficile bilanciamento tra il diritto di cronaca e il diritto all'oblio: la soluzione delle sezioni unite*; in *Giustizia civile. com*, 24 marzo 2020, con nota di A. R. Rizza, *Lucciole per lanterne. La n. 19681 del 2019 e la terra promessa del diritto all'oblio*; in *Giurisprudenza costituzionale*, 1, 2020, 349 ss., con nota di M. Mezzanotte, *Il diritto all'oblio secondo le Sezioni Unite: cerbero o chimera?*

[58] Cass. civ., sez. un., 22 luglio 2019, n. 19681, cit., § 9.

[59] I n tal senso R. Pardolesi, ult. cit., c. 3086.

nel 2001 sul sito del *New York Times*[60]; tale scritto, riportando alcuni rapporti del FBI (risalenti al 1994) e delle forze dell'ordine europee, mirava a evidenziare i presunti, passati legami del ricorrente con la criminalità organizzata russa. Conscio dell'elevato *standard* di tutela assicurato dal Primo Emendamento della Costituzione americana alla libertà di parola, lo stesso Fuchsmann aveva radicato il giudizio in Germania (giustificando la competenza della Corte tedesca tanto mediante la presenza di copie cartacee del quotidiano presso le librerie di Düsseldorf, quanto attraverso l'accessibilità internazionale della sua versione online), senza tuttavia che le sue richieste fossero accolte. La Corte EDU, chiamata a verificare il corretto bilanciamento fra il diritto al rispetto della vita privata tutelato dal succitato art. 8 CEDU e quello alla libertà d'espressione salvaguardato dall'art. 10 CEDU, riteneva che tale attività interpretativa dovesse essere guidata dal rispetto di cinque parametri (fonte di ispirazione per la Cassazione italiana, che a tali indici ha fatto espresso richiamo nella già ricordata sentenza n. 6919 del 2018): a) il contributo offerto dall'articolo al dibattito pubblico; b) la notorietà del soggetto interessato; c) il metodo adottato per ottenere le informazioni e verificarne la veridicità; d) la condotta del soggetto precedente alla pubblicazione dell'articolo o il fatto che le informazioni contestate fossero già state diffuse in altra sede; e) il contenuto e la forma della pubblicazione, nonché le conseguenze da essa prodotte. Accertato che, senza operare insinuazioni e facendo affidamento su fonti attendibili, l'articolo del quotidiano statunitense riguardava unicamente la vita professionale del ricorrente e che il coinvolgimento di quest'ultimo nell'elezione del sindaco di New York – sospettato di corruzione – aveva reso nuovamente attuale l'interesse dell'opinione pubblica sul suo conto (rendendo così irrilevante il rilievo del lungo tempo intercorso fra l'epoca dei fatti narrati e quella della loro reclamizzazione), la Corte escludeva la violazione dell'art. 8 CEDU[61]. Ancor più significativa è una recentissima decisione del medesimo consesso nel caso *Biancardi c. Italia*[62]. Il ricorrente, *ex* caporedattore di un giornale online, era stato ritenuto responsabile in sede civile a fronte della mancata deindicizzazione dei *tag* di un articolo riguardante l'episodio di una rissa in un ristorante (poi degenerata in un accoltellamento), corredato fra l'altro da dettagli riguardanti i relativi procedimenti penali nel frattempo avviati. Secondo Strasburgo, la pronuncia del giudice nazionale non avrebbe violato l'art. 10 CEDU, tenuto conto del considerevole lasso di tempo durante il quale l'articolo era rimasto accessibile, della facile reperibilità del medesimo e soprattutto della natura privata dei soggetti coinvolti (dei quali erano state diffuse le generalità e le rispettive vicende giudiziarie in corso). Oltre a confermare la validità dei

[60] CEDU, *Fuchsmann c. Germania*, ric. n. 71233/13, (2017), in *Diritto penale contemporaneo*, 4, 2018, 215 ss., con nota di E. Mazzanti, *Vecchio sospetto di reato e diritto all'oblio. A proposito di una recente sentenza della Corte di Strasburgo*; in *Danno e responsabilità*, 2018, 149 ss., con nota di S. Bonavita - R. Pardolesi, *La Corte Edu contro il diritto all'oblio?*

[61] In senso conforme, si segnalano le pronunce rese sui casi CEDU, *Axel Springer AG c. Germania*, ric. n. 39954/08, (2012); CEDU, *von Hannover c. Germania*, ricc. nn. 40660/08 e 60641/08, (2012); CEDU, *Couderc and Hachette Filipacchi Associès c. Francia*, ric. n. 40454/07, (2015).

[62] CEDU, *Biancardi c. Italia*, ric. n. 77419/16, (2021), in *Giustizia civile.com*, 22 dicembre 2021, con nota di A. Malafronte, *Libertà di informazione e* deindexing *nel caso Biancardi c. Italia*. Il testo è disponibile all'indirizzo *giustiziacivile.com*. Particolarmente critico è il giudizio offerto da A. Monti, *La Corte europea dei diritti umani riconosce il diritto a cancellare la storia*, in *la Repubblica*, 3 dicembre 2021, disponibile all'indirizzo *repubblica.it*.

criteri già elaborati nel caso *Fuchsmann*, la Corte ha espresso in questa sede una considerazione di particolare momento, ritenendo che l'obbligo di deindicizzazione, oltre a essere imposto al gestore di un motore di ricerca (come statuito dalla Corte di Giustizia dell'Unione Europea nella vicenda *Google Spain*), possa essere adempiuto anche da «amministratori di giornali o archivi giornalistici accessibili tramite Internet»[63]. Tale pronuncia si concilia con la soluzione raggiunta dalla Corte di Cassazione pochi mesi prima[64], la quale, confrontandosi con il caso di un articolo online che aveva riportato il contenuto di alcune intercettazioni telefoniche cui non era seguita l'apertura di alcun procedimento penale nei confronti dell'interessato (nello specifico, un imprenditore – noto unicamente a livello locale – ritenuto vicino ad ambienti massonici e sodalizi mafiosi), aveva riconosciuto il suo diritto alla deindicizzazione di tali contenuti, non rivestendo quest'ultimo la qualifica di personaggio pubblico a livello nazionale. Proprio il mancato riscontro di una tale notorietà, infatti, non giustificherebbe la persistente indicizzazione di una «biografia telematica, diversa da quella reale e costituente oggetto di notizie ormai superate»[65], e ciò anche nel caso le notizie stesse non ineriscano episodi particolarmente lontani nel tempo.

La particolare attenzione riservata al requisito della notorietà stimola, in conclusione, un commento che in alcun modo intende svalutare gli sforzi dei giudici impegnati in questioni così spinose, posta l'impossibilità di pervenire alla quadratura di un cerchio quale quello rappresentato dai confini del diritto all'oblio: pur essendo pienamente comprensibile che un individuo particolarmente popolare sia chiamato a tollerare un grado di ingerenza nella sua vita privata superiore a quello subito dal *quisque de populo*, l'opposta prospettiva - percepibile osservando la giurisprudenza degli ultimi anni - che la minore celebrità di un soggetto possa quasi automaticamente giustificare la deindicizzazione dei contenuti a lui attribuibili suscita più di una perplessità. È comprensibile interrogarsi se gli utenti operanti nella sua stessa area geografica non possano vantare un diritto all'informazione pari a quello dei fruitori di quotidiani a stampa od online che desiderino conoscere le gesta di una persona nota in tutta la Penisola ma caratterizzata da una simile se non identica pericolosità sociale. A titolo puramente esemplificativo, apprendere informazioni concernenti un tale modello di cittadino, pur ignoto ai più, ben può essere giustificato da ragioni di ordine pubblico, in questo caso inteso quale garanzia di sicurezza e serenità da parte dei consociati. Per questa ragione, a fronte della già segnalata mancanza di indicazioni circa il congiunto rispetto dei parametri definiti dai "decaloghi" poc'anzi osservati, pare ragionevole affermare come il requisito dell'interesse pubblico (indifferentemente nazionale o locale) debba rivestire un peso specifico maggiore rispetto a quelli della notorietà e del tempo trascorso dalla data di verificazione dei fatti narrati.

---

63 Ivi, § 51 (traduzione a cura dello scrivente, n.d.r.).

64 Cass. civ., sez. I, ord. 31 maggio 2021, n. 15160, in *Il Foro italiano*, 2022, c. 320 ss., con nota di A. Palmieri, *Diritto all'oblio, deindicizzazione e conclusioni non consequenziali alle premesse.*

65 *Ibid.*

4. Il diritto all'oblio tratteggiato dalla Riforma Cartabia

Posta l'imprescindibile rassegna normativa e giurisprudenziale finora svolta, nuovi spunti di riflessione in materia di deindicizzazione di informazioni contenute in provvedimenti giurisdizionali sono oggi stimolati dal nuovo art. 64-*ter* disp. att. c.p.p. ("Diritto all'oblio degli imputati e delle persone sottoposte ad indagini") introdotto dal d.lgs. 10 ottobre 2022, n. 150[66], fra le disposizioni meno reclamizzate nell'alveo della vasta Riforma Cartabia approvata in esame definitivo il 28 settembre scorso. L'entrata in vigore della stessa, originariamente prevista per il 1° novembre 2022, è stata prorogata al 30 dicembre 2022 per effetto dell'art. 6 del D.L 31 ottobre 2022, n. 162.
In ossequio ai criteri direttivi espressi nella l. 27 settembre 2021, n. 134 (*Delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari*), che al suo art. 1, c. 25 esortava il Governo a «prevedere che il decreto di archiviazione e la sentenza di non luogo a procedere o di assoluzione costituiscano titolo per l'emissione di un provvedimento di deindicizzazione che, nel rispetto della normativa dell'Unione europea in materia di dati personali, garantisca in modo effettivo il diritto all'oblio degli indagati o imputati»[67] (creando così una "via diretta" rispetto a quelle rappresentate dall'attesa di un provvedimento del Garante privacy o del giudice civile), l'esecutivo ha previsto al succitato art. 64-*ter* disp. att. c.p.p. che «l'imputato destinatario di una sentenza di proscioglimento o di non luogo a procedere e la persona sottoposta alle indagini destinataria di un provvedimento di archiviazione possono richiedere che sia preclusa l'indicizzazione o che sia disposta la deindicizzazione, sulla rete internet, dei dati personali riportati nella sentenza o nel provvedimento, ai sensi e nei limiti dell'art. 17 del regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016. Resta fermo quanto previsto dall'articolo 52 del decreto legislativo 30 giugno 2003, n. 196». I commi secondo e terzo affermano poi come, tanto nel caso di richiesta volta a precludere l'indicizzazione quanto di quella tesa a ottenere la deindicizzazione, la cancelleria del giudice che ha emesso il provvedimento sia chiamata ad apporre e sottoscrivere una dichiarazione recante il riferimento al suddetto art. 17 GDPR; più nel dettaglio, mentre il c. 2 vieta «l'indicizzazione del [ ] provvedimento rispetto a ricerche condotte sulla rete internet a partire dal nominativo dell'interessato», il c. 3 parla di un «provvedimento di sottrazione dell'indicizzazione, da parte dei motori di ricerca generalisti, di contenuti relativi al procedimento penale, rispetto a ricerche condotte a partire dal nominativo dell'istan-

[66] Attuazione della legge 27 settembre 2021, n. 134 recante delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari, Gazzetta Ufficiale n. 243 del 17 ottobre 2022.

[67] L. 27 settembre 2021, n. 134 (Delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari), Gazzetta Ufficiale n. 237 del 4 ottobre 2021. Un primo commento è stato offerto da A. Procaccino, *Oblio e deindicizzazione nella delega Cartabia: rose e spine*, in *Giurisprudenza italiana*, 2022, 1028 ss. In particolare, M. Pisapia - C. Cherchi, *Diritto all'oblio. Prime riflessioni sull'introduzione dell'art. 64-ter disp. att. c.p.p.*, in *Giurisprudenza italiana*, 3, 2022, 337 ss. hanno sottolineato come «la norma sembra inscriversi nel più ampio percorso intrapreso dal nostro legislatore – su spinta comunitaria – di rafforzamento della tutela dei diritti dell'indagato/imputato in un'ottica extra-processuale», individuando nell'attuazione della direttiva (UE) 343/2016 sulla presunzione di innocenza il primo significativo intervento in tale direzione.

te». Nell'ampia relazione illustrativa al decreto, il legislatore delegato ha avuto modo di spiegare le proprie linee d'intervento: fra di esse, il fatto che la locuzione "costituire titolo" adottata dal delegante lasci «intravedere una iniziativa su richiesta - ed in tal senso si è operato - che esclude l'attivazione officiosa o comunque automatismi incombenti sulle cancellerie»[68].

Fra le osservazioni formulabili, merita in primo luogo di essere rilevato come il legislatore delegante abbia indirizzato l'operato del delegato optando per la deindicizzazione (in luogo della ben più netta cancellazione), dimostrando così particolare attenzione verso l'interpretazione e l'evoluzione del diritto all'oblio a partire dalle già esaminate pronunce della Corte di Giustizia dell'Unione Europea. Le ragioni di tale soluzione mediana[69] vanno con ogni probabilità ravvisate nel fatto che l'art. 64-*ter* disp. att. c.p.p. non richiede il passaggio in giudicato dei provvedimenti giurisdizionali menzionati[70], da cui il possibile, successivo intervento di provvedimenti di segno opposto: mentre la sentenza di assoluzione può essere ribaltata in appello, l'impugnazione di quella di non luogo a procedere è oggi soggetta alle condizioni dettate dal nuovo art. 554-*quater* c.p.p.; lo stesso può considerarsi in relazione al decreto di archiviazione, la cui stabilità può essere minata da quella «esigenza di nuove investigazioni» cui l'art. 414 c.p.p. subordina la riapertura delle indagini. La previsione di un'aprioristica deindicizzazione estesa anche ai provvedimenti resi all'esito degli eventuali, successivi giudizi d'impugnazione, oltre a tradire il contenuto del succitato art. 1, c. 25 (da cui la prospettiva di un eccesso di delega), avrebbe di fatto impedito qualunque ulteriore bilanciamento fra il diritto del singolo e quello della collettività alla conoscenza del procedimento penale, soprattutto rispetto a vicende giudiziarie in cui l'interesse dei consociati, inizialmente modesto o addirittura insussistente in ragione di un esito giudiziario favorevole all'indagato/imputato, assuma consistenza in relazione a fattori quali l'intervento di "svolte" nel corso del medesimo.

In seconda istanza, la norma in esame identifica il destinatario della richiesta di deindicizzazione nella figura del gestore del motore di ricerca (adottando la locuzione «mo-

[68] Supplemento straordinario n. 5 alla Gazzetta Ufficiale n. 245 del 19 ottobre 2022, 348.

[69] Per una lettura della deindicizzazione quale soluzione di compromesso, v. da ultimo Cass. civ., sez. I, 8 febbraio 2022, n. 3952: «La deindicizzazione dei contenuti presenti sul web rappresenta, il più delle volte, l'effettivo punto di equilibrio tra gli interessi in gioco. Essa integra, infatti, la soluzione che, a fronte della prospettata volontà, da parte dell'interessato, di essere dimenticato per il proprio coinvolgimento in una vicenda del passato, realizza il richiamato bilanciamento escludendo le estreme soluzioni che sono astrattamente configurabili: quella di lasciare tutto com'è e quella di cancellare completamente la notizia dal web, rimuovendola addirittura dal sito in cui è localizzata» (occasione nella quale la Suprema Corte, pur accogliendo una richiesta di deindicizzazione, ha invece rigettato quella di cancellazione degli URL indicati nel ricorso e delle copie *cache* delle pagine accessibili attraverso di essi, ritenendo la cancellazione stessa eccessiva in quanto lesiva del diritto della collettività a essere informata).

[70] Il legislatore delegato, nel già citato Supplemento straordinario n. 5 alla Gazzetta Ufficiale n. 245 del 19 ottobre 2022, 349, ha offerto alcuni chiarimenti quanto alla corretta interpretazione delle formule "decreto di archiviazione", "sentenza di non luogo a procedere" e "sentenza di assoluzione" originariamente adottate dal delegante: «non avrebbe senso, da un lato, includere i decreti ed escludere le ordinanze di archiviazione; dall'altro, includere le sentenze dibattimentali di assoluzione (art. 530) ed escludere quelle dibattimentali di non doversi procedere (artt. 529 e 531), quando le archiviazioni e le sentenze di non luogo a procedere vengono menzionate abbracciando qualunque "formula". Nel comma 1 della norma […] si sono apportate, pertanto, le opportune formule armonizzatrici [= sentenza di proscioglimento o di non luogo a procedere e provvedimento di archiviazione]».

tori di ricerca generalisti»), con ciò uniformandosi ai principi espressi nel già affrontato caso *Google Spain* (*supra*, par. 3.1.); tuttavia, nei mesi precedenti all'intervento del legislatore delegato era stato segnalato «come, da un punto di vista operativo, sia i social network che le testate giornalistiche online operino con capacità tecniche (impensabili fino a 10 anni fa) in grado di immagazzinare e ritenere enormi archivi informatici, che consentono una capillare *searchability* e filtrabilità dei contenuti»[71]. Un simile ampliamento del novero dei soggetti raggiunti da un obbligo di deindicizzazione, il quale pare riecheggiare le considerazioni svolte sul punto dalla Corte di Strasburgo nel caso *Biancardi c. Italia* (*supra*, par. 3.2.), avrebbe potuto realizzarsi almeno per quanto riguarda le testate giornalistiche, considerato come l'art. 85, par. 2, GDPR, relativo a ipotesi di trattamento dei dati «effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria», consenta agli Stati membri di prevedere esenzioni o deroghe rispetto ai principali Capi del regolamento stesso (tanto più se si considera che il destinatario della richiesta, lungi dall'essere espressamente indicato dall'art. 17 GDPR, è stato a oggi individuato in via puramente giurisprudenziale a partire dal summenzionato caso *Google Spain*). Al netto dell'opinione espressa dalla dottrina giuridica, l'attuabilità dell'estensione in parola, tale da includere nuovi soggetti nella platea dei recettori di una richiesta di deindicizzazione, imporrebbe inevitabilmente un previo dialogo con la scienza informatica, la sola in grado di chiarire se i *social network* e i quotidiani digitali possiedano a oggi tecnologie tali da poter intervenire con la stessa esperienza e organizzazione di un motore di ricerca "generalista".

Ancora, l'art. 64-*ter* disp. att. c.p.p., ai suoi commi 2 e 3, si premura di specificare l'oggetto della deindicizzazione, colmando in tal senso una significativa lacuna ravvisabile in seno alla delega: mentre la domanda di preclusione all'indicizzazione concerne il provvedimento nel suo insieme, la richiesta di deindicizzazione riguarda più ampiamente i «contenuti relativi al procedimento penale» nel frattempo circolati in Rete. In tal senso, mentre la prima annotazione è espressione di una tutela anticipata, tesa a precludere la diffusione del provvedimento (non potendosi in tal caso parlare di vero e proprio "oblio", trattandosi di dati personali mai usciti dai palazzi di giustizia e, quindi, mai conosciuti dalla collettività), la seconda operazione, di carattere rimediale, comporta uno sforzo particolarmente significativo, posto come la formula da ultimo richiamata evochi il *mare magnum* di informazioni accumulatesi online in assenza di una previa preclusione all'indicizzazione del provvedimento[72]. In entrambi i casi, il conclu-

[71] A. Procaccino, *Oblio e deindicizzazione nella delega Cartabia*, cit., 1029. In alternativa, l'Autrice prospettava «un obbligo di aggiornamento e adeguamento della "storia processuale" da imporre alle testate» (p. 1030). Tale suggestione rievoca il tema della storiografia giornalistica e della gestione degli archivi storici, cui si è già fatto riferimento citando la giurisprudenza di cui *supra*, par. 3.

[72] In tal senso, il legislatore delegato ha accolto le indicazioni offerte dal Garante privacy allo schema di decreto con comunicato stampa del 16 settembre 2022 ("Garante privacy: ok alla riforma del processo penale. Suggerite tutele per la maggiore riservatezza degli atti giudiziari e nuove forme di diritto all'"oblio"): l'Autorità, infatti, proponeva «di introdurre più incisive tutele per le persone destinatarie di provvedimenti di archiviazione o proscioglimento, definendo due nuove forme di "oblio", peraltro in linea con il principio costituzionale della presunzione di innocenza. Una prima forma di "oblio" dovrebbe garantire la deindicizzazione preventiva dei provvedimenti giudiziari in modo da sottrarre il nome di indagati e imputati alle ricerche condotte tramite motori generalisti; una seconda forma dovrebbe intervenire, invece, nella fase successiva consentendo ai soggetti coinvolti di richiedere la sottrazione all'indicizzazione, *ex post*, dei propri dati contenuti nel provvedimento». Il testo del

sivo richiamo alle ricerche condotte a partire dal nominativo dell'istante è un chiaro riferimento alle indicazioni offerte sul punto nei casi *Google Spain* e *Google 2*, occasione in cui i giudici sovranazionali, vagliando l'origine delle ricerche i cui risultati erano stati oggetto di una richiesta di deindicizzazione, avevano constatato come la stessa risiedesse nelle generalità dell'interessato.
Un ultimo quesito sorge in relazione ai mezzi di tutela invocabili nel caso di mancato rispetto degli adempimenti prescritti dalla norma, nonché al regime di responsabilità conseguente a tale inerzia. Sul punto, la norma rimane silente. A ben vedere, l'automatismo dell'annotazione di non indicizzazione o deindicizzazione quale conseguenza del deposito di uno dei provvedimenti presupposto non riguarda il giudice, bensì il cancelliere, normalmente soggetto a responsabilità civile (nelle ipotesi regolate dall'art. 60 c.p.c.), penale (*ex* art. 328 c.p., qualora la sua condotta integri il delitto di rifiuto od omissione di atti d'ufficio) e disciplinare (ai sensi dell'art. 104 della l. 23 ottobre 1960, n. 1196). Oltre a ciò, ci si domanda di fronte a quale autorità editori e giornalisti, interessati alla diffusione di notizie concernenti un procedimento penale, potranno presentare un'opposizione alle annotazioni stesse, sempre che la disposizione in esame non intenda nella sua asciuttezza precludere a monte una simile eventualità.

5. Conclusioni

All'esito di una riflessione finalizzata a delineare un panorama esaustivo della tutela dei dati personali nell'ambito di procedimenti penali, la complessità e l'ardua riconducibilità a sistema degli istituti trattati rendono ineludibili alcune considerazioni finali.
Se l'art. 52 del d.lgs. 30 giugno 2003, n. 196 e la nozione di "motivi legittimi" da esso recata non hanno a oggi fatto registrare particolari criticità applicative (come attestato dalla poca e complessivamente concorde giurisprudenza sul tema), il diritto all'oblio pone come osservato alcuni quesiti quanto al rilievo dei suoi singoli requisiti operativi, alle facoltà attraverso cui può esprimersi nonché ai soggetti chiamati a garantirne la concreta attuazione. Constatata la centralità e l'assenza di contraltari all'art. 17 GDPR, imprescindibile parametro normativo cui il legislatore italiano non ha potuto discostarsi in occasione della recentissima riforma del processo penale (e da cui, inevitabilmente, dipenderà l'effettiva portata applicativa dell'art. 64-*ter* disp. att. c.p.p.[73]), occorre anzitutto ricordare come l'espresso, esclusivo riferimento al concetto di "cancellazione" abbia generato significativi dubbi interpretativi, specie se rapportato a espressioni erroneamente ritenute sinonimiche: conferma di quanto appena osservato si ha per

comunicato è disponibile all'indirizzo *garanteprivacy.it*.

[73] A ben vedere, il disposto dell'art. 64-*ter* disp. att. c.p.p. «non presenta carattere realmente innovativo», limitandosi infatti a cristallizzare una prassi costante del Garante privacy in base a cui «l'esito favorevole del procedimento penale (e, per l'Autorità, persino il riconoscimento del beneficio della non menzione della sentenza di condanna) assurge a parametro rilevante, da considerare ai fini della decisione dell'istanza di deindicizzazione». Così il Parere sullo schema di decreto legislativo di attuazione della legge 27 settembre 2021 n. 134, recante delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari, doc. web n. 9802612 del 1° settembre 2022, disponibile all'indirizzo *garanteprivacy.it*.

voce dei giudici di Strasburgo, i quali hanno rilevato come i termini *de-indexing*, *de-listing* e *de-referencing* «siano spesso utilizzati in maniera intercambiabile in diverse fonti dell'Unione Europea e del diritto internazionale, e che il loro significato specifico può spesso essere tratto solo dal contesto in cui sono utilizzati»[74]. Oltre a ciò, va ammesso come particolari difficoltà sorgano dal fatto che il tema mal si presti a un approccio sistematico, come attestato da alcune insormontabili divergenze sorte fra gli esegeti delle norme a tutela della privacy (si pensi a quelle riguardanti gli archivi storici e, di riflesso, la pratica della storiografia giornalistica) e dal pericolo di un'eccessiva fedeltà e prevalenza accordata ad alcuni parametri di quei "decaloghi" originati in seno alle pronunce esaminate nel corso del presente contributo. In questi termini, il bilanciamento del diritto all'oblio con quello alla cronaca è destinato a rimanere un'attività dinamica, alieno a moduli predefiniti e irrimediabilmente tarato in relazione al caso di specie.

Con specifico riferimento alla deindicizzazione, concetto cardine intorno a cui si impernia la disposizione introdotta dalla Riforma Cartabia, i maggiori timori continuano a essere suscitati dall'investitura del gestore del motore di ricerca quale arbitro nella valutazione di simili istanze e, conseguentemente, nella selezione delle informazioni da deindicizzare, ribadendosi in tal senso quanto si è già avuto modo di commentare in relazione al caso *Google Spain*: se da un lato il gestore stesso si presenta quale recettore prediletto delle richieste in virtù del controllo esercitato sul proprio motore di ricerca e della disponibilità dei mezzi informatici necessari per compiere tali operazioni, dall'altro paiono giustificati i timori di giudizi arbitrari o fra loro incoerenti, posto come gli interessi di un soggetto privato ben possano divergere dagli obiettivi che ispirano un ordinamento giuridico statale. Di conseguenza, la predisposizione da parte di Google di un apposito "modulo per la richiesta di rimozione di dati personali"[75], corredato da una sintetica indicazione dei motivi per cui la richiesta medesima potrebbe incontrare il rifiuto del gestore del motore di ricerca[76], si rivela in realtà una foglia di fico, risultando *de facto* vanificata dall'imperscrutabilità dei giudizi in questione.

[74] *Biancardi c. Italia*, cit., § 53 [traduzione a cura dello scrivente, n.d.r.].

[75] Il modulo messo a disposizione dalla società di Mountain View è disponibile all'indirizzo *reportcontent.google.com*.

[76] Nel caso di Google, il richiamo è a informazioni riguardanti frodi finanziarie, negligenza professionale, condanne penali o "la condotta pubblica di funzionari governativi".

Complexity of IoT technologies: European regulations in progress and patterns of customer communication*

Chiara Vescovi

Abstract

Internet of Things devices generate ecosystems that enter the households of customers and influence their everyday life. Therefore, in building these technologies, manufacturers are called upon to assess the cultural and digital context and the effect of digitalisation in end-users, who expect products to be trustworthy, safe, and compliant with the needs brought up by a fast-changing digital world. The European Union is adopting a multidisciplinary approach in the attempt to regulate a highly horizontal matter, impacting people and markets. The article analyses the last legislative proposals, balancing the right of consumers and the efforts required to manufacturers to comply with a responsible approach to these technologies. Building a trusting communication channel between stakeholders may be the only feasible approach, as legislative solutions can help but rarely will be (alone) able to solve all issues related to such a pervasive technology.

I dispositivi connessi generano ecosistemi di prodotti e funzionalità che entrano nella quotidianità e nelle dimore dei consumatori. Pertanto, i produttori vengono chiamati a rispondere non solo della conformità dei prodotti, ma anche a considerare il contesto culturale e digitale nel quale essi sono inseriti e gli effetti della digitalizzazione sui consumatori finali, che si abituano a confrontarsi con un mondo che cambia di pari passo con la tecnologia. Nel tentativo di regolare al meglio un fenomeno che impatta cittadini e mercati, l'Unione Europea adotta un approccio multidisciplinare, che l'articolo si propone di ripercorrere. L'analisi si concentra sugli investimenti richiesti ai produttori di tecnologia IoT per realizzare dispositivi che rispettino i criteri di responsabilità e i diritti dei consumatori. La soluzione proposta è la costituzione di un canale comunicativo e di fiducia tra produttori e consumatori, che sia complementare a soluzioni legislative non sempre soddisfacenti in caso di tecnologie così innovative e pervasive.

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

Summary

Keywords

Internet of Things - Artificial Intelligence - Data Act - European Union - consumer protection

1. Regulating the Internet of Things: A European perspective

When computing and smart devices are synchronized with physical hardware the output generated is known as Internet of Things[1] (or IoT) as the «connection between the physical and the cyber systems allows a seamless transfer of data (through network connectivity) without any interference from users».[2]

Mankind has always had the tendency to substitute manpower with machines when a person providing a task resulted less efficient and slower than a machine.[3] This attitude is a direct consequence of a technical and technological revolution which had been going on for years and, understandably, experienced an acceleration in the past years with the advancement of studies in Machine Learning and Artificial Intelligence, making data analytics more common, easier, and referred to a larger quantity of data.[4]

The attractiveness of the IoT technology goes back to 1970s when it was known as "embedded internet". [5] Pushed by large commercial giants such as Procter and Gamble, Google, and Gartner[6] it had various instant of glories up until today, when learning technologies entered our everyday life and our households through supports such as smart home assistants and the wearable devices. IoT applications are invading many different areas of our everyday life: affecting education[7], driving, cooking, sport

[1] F. Gregorio et al., *Internet of things in Signal Processing Techniques for Power Efficient Wireless Communication Systems*, New York City, 217 ss.

[2] A. Saeed et al., *Energy Efficient Hybrid IoT System for Ambient Living,* Switzerland, 2022.

[3] N. Wiener, *The Human use of Human Beings – Cybernetics and Society*, Cambridge, 1950.

[4] R. Khan, *Future internet: the internet of things architecture, possible applications and key challenges*, 257 ss.

[5] A. Saeed, *A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems*, 18.

[6] A. Saeed, *A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems*, cit.

[7] I. N. Mseer, *Internet of Things and Its Impact on the Future of Education*, Switzerland, 2021.

and living; but became also a valuable support to improve system reliability, security and safety thanks to predictive maintenance, statistical analysis, and estimations.[8]
Advanced technologies introduced models and standardisation[9] into our reality: reproducing and ameliorating human patterns that have been studied and analysed deeply. Standards provide use cases for rules, harmonize requirements and «even more than general standards, ICT standards have a vital economic interest as they foster progress in creating more efficient and interoperable components of new technological objects. However, they can also constitute a barrier to the market»[10] therefore legislators shall be aware of the burden that standards bring with them.

1.1. The beginning

The European Commission interest in IoT and its legislative perspective goes way back and already in 2009, it addressed Internet of Things as "an umbrella for a new paradigm."[11] An emerging interest for the protection of personal data and awareness in dealing with technical innovations (which were, indeed, about to become some of the main concerns of the European Union) contributed to the popularity of the IoT conversations. Reasonings and studies on the best way to deal with new technologies kept flowing and scholars started to deliver some requirements that would have had to be kept in mind in regulating the Internet of Things.[12]
Among others, in 2010 Professor Rolf H. Weber listed four characteristics of IoT[13] that must be considered when dealing with this type of technology: understanding them is intrinsically linked to a correct governance of their inputs and outcomes.

- *Globality*, i.e., the trans-border element, embedded in products and services connected with networks.
- *Verticality*, meaning the durability of the products, which if connected can usually be updated and therefore extend their lifespan through upgrades and more efficient algorithms.
- *Ubiquity*, referring to the fact that the same product or service can be accessed simultaneously by different persons and from different places.
- *Technicity,* which stands for the necessity to consider the technical complexity of the devices connected.

New rules and legislations that are spawning within the EU institutions shall consider

[8] B.C. Kavitha - R. Vallikannu, *Fault Detection and Data Management for IoT*, in *Multimedia Technologies in the Internet of Things Environment*, 93, Singapore, 147 ss.

[9] F. Gennari*, Standard Setting in Organitsations for the IoT: How to Ensure a Better Degree of Liability?,* in *Masaryk University Journal of Law and Technology*, 15, 2021, 153 ss.

[10] Ivi, 155.

[11] Commission of the European Communities, *Communication from the Commission to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions*, Internet of Things — An action plan for Europe.

[12] R. H. Weber, *Internet of Things – New security and privacy challenges*, in *Computer Law & Security Review*, 26, 2010, 23 ss.

[13] R. H. Weber, *Internet of Things – New security and privacy challenges*, cit., 23-30.

the previous as a common ground on which building provisions that are adaptable with innovations connected with this technology.

1.2. The European answer to a business opportunity

Besides being instruments of efficiency and development, nowadays IoT devices represent an almost irreplaceable asset for companies, as they «will [keep] foster[ing] an exponential growth in the volume, quality, and variety of consumer-generated data».[14] Moreover, the "monetary value" of consumer data[15] increases the larger the number of data processed, as «informational goods are non-rival in nature. Hence, economic welfare will typically increase by data sharing».[16]

The vastity of the market surrounding IoT devices was confirmed in 2022 by the European Commission that in its final report on consumer Internet of Things affirmed that:

«As the use of consumer IoT products is increasingly becoming part of everyday life for Europeans, the consumer IoT sector is expected to grow significantly in the coming years. It is predicted that overall consumer IoT revenue worldwide will grow from EUR 105.7 billion in 2019 to approximately EUR 404.6 billion by 2030. European smart home revenue will also more than double between 2020 and 2025 (from approximately EUR 17 billion to approximately EUR 38.1 billion)[17]».

Such economic value shall be supported by a solid legislative framework, able to enhance the business development while protecting the rights of citizens and consumers. Therefore, it is no coincidence that, looking at the legal initiatives the European Union is working on, some documents seem to be destined to have a calculated interest in the IoT market.

In the present paper some of the initiatives proposed by the Union will be analysed more in depth, to better understand their value for IoT technologies. They are:

- The proposal for a Data Act[18], a programmatic document which aims at governing data generated by IoT devices, with a strategic approach.
- Two cybersecurity initiatives:
    - the Cybersecurity Act[19], in force since 2019, which established a European cybersecurity certification scheme managed by the European Union Agen-

[14] S. Elvy, *A commercial law of privacy and security for the internet of things*, Cambridge, 2021, 244.

[15] P. M. Schwartz, *Property, Privacy and Personal Data*, in *Harvard Law Review*, 117, 2004, 2055 ss.

[16] J. Drexl, *Access as a Means to Promote Consumer Interests and Public Welfare – An Introduction* in *German Federal Ministry of Justice and Consumer Protection,* Max Planck Institute for Innovation and Competition (eds.), Data Access, Consumer Interests and Public Welfare, Baden-Baden 2021, 11 ss.

[17] European Commission, Final Report from the Commission to the Council and the European Parliament – *Final report – sector inquiry into consumer Internet of Things*.

[18] Proposal for a Regulation of The European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).

[19] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

cy for Cybersecurity (ENISA).

- The proposal for a Cyber Resilience Act[20], which aims at harmonising cybersecurity rules for products with digital elements, therefore tackling Internet of Things products specifically.

- A new framework on civil liability:
  In this context the Union looked at Artificial Intelligence, IoT and robotics together, as they share some main characteristics that have led the European legislator to combine the analyses and legislative interventions. The framework represents a package of legal actions with the purpose of raising trust towards AI-related products at the Union level and ensuring that remedies and actions for damages are accessible to final consumers. The framework includes:
  - The proposal for an AI Liability Directive[21], aiming at adapting non-contractual civil liability rules to artificial intelligence.
  - The proposal for a renewed Product Liability Directive[22], dealing with liability for defective products: in the proposal the scope of the Directive has been extended to include digital products and it considers them within the context of circular economy, expanding the responsibility of manufacturers.
- The Ecodesign and Energy Labelling – Framework Directives[23], two Directives tackling energy-using products (EUPs), among which it is possible to classify Internet of Things products. The Framework is addressed to highlight some information requisites placed on manufacturers.

2. European legislative initiatives to regulate the Internet of Things

2.1. Governance and Strategy

IoT data governance can be challenging as Internet of Things devices involve different kind of data: personal data of the final user (which are protected by the provisions of the General Data Protection Regulation) and non-personal data, that are generated by the very use of the device[24]. These data mainly remain in control of the manufac-

[20] European Commission, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act).

[21] European Commission, Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive).

[22] European Commission, Proposal for a Directive of the European Parliament and the Council on liability for defective products, (Product Liability Directive).

[23] The Framework comprehends: Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products; Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 setting a framework for energy labelling and repealing Directive 2010/30/EU.

[24] W. Kerber, *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, in *GRUR International*, 2023, 72(2), 120 ss.

turer who designed the product, usually giving little to no access to consumers to the generated information.

2.1.1. The Data Act

The proposal for a Regulation on harmonised rules on fair access to and use of data was adopted by the Commission on February 23rd, 2022, and it marks a fundamental pillar of the Digital Decade.[25] It is set to bring fairness into the technological perspectives by setting up provisions on how to use and process data generated by Internet of Things Devices.

The Proposal introduces:

- «Measures to allow users of connected devices to gain access to data generated by them […]; and to share such data with third parties to provide aftermarket or other data-driven innovative services. It maintains incentives for manufacturers to continue investing in high-quality data generation, by covering their transfer-related costs and excluding use of shared data in direct competition with their product.
- Measures to rebalance negotiation power for SMEs by preventing abuse of contractual imbalances in data sharing contracts. […]
- Means for public sector bodies to access and use data held by the private sector that is necessary for exceptional circumstances, particularly in case of a public emergency […]
- New rules allowing customers to effectively switch between different cloud data-processing services providers and putting in place safeguards against unlawful data transfer»[26].

On December 2022 a compromise text was discussed by the EU Council, extending its entry into application from the original 12 months to 18 months.[27] The transition in the past months within the EU Council from the Czech presidency to the Swedish presidency, to the Spanish presidency seems to have enhanced the urgency of the document, making it a priority.[28] In mid-March the European Parliament's voted in plenary session to approve their version of the Data Act, opening the door to interinstitutional discussions with the EU Council and Commission. In June 2023 a political agreement was reached on the document. Significant proposals have been introduced to increase transparency for the manufacturers and to regulate B2B data transfers.[29] The new rules are awaited with some excitement by Member States as they shall create and additional GDPR of €270 billion by 2028 by tackling the legal, economic and

[25] European Commission, *Shaping's Europe Digital Future – Data Act*.

[26] European Commission, *Press Release - Data Act: Commission proposes measures for a fair and innovative data economy*, 23 February 2022, available at *ec.europa.eu*.

[27] L. Bertuzzi, *EU Council set to revise cloud-related provisions in new data law*, in *EURACTIV*, 9 December 2022 (updated on 13th December 2022), available at *euractiv.com*.

[28] L. Bertuzzi, *Swedish presidency offers EU countries options on Data Act's pain points*, in *EURACTIV*, 12 January 2023 (updated on 13th January 2023), available at *euractiv.com*

[29] L. Bertuzzi, *EU lawmakers formalise position on the Data Act in plenary vote*, in *EURACTIV*, 14 March 2023 (updated on 16th March 2023), available at *euractiv.com*.

technical reasons that lead to a limited use of some data.[30]

The proposal is consistent with existing rules on the use of personal data (addressed by the General Data Protection Regulation[31]) and non-personal data (regulated by the Free Flow of Non-Personal Data Regulation[32]), but also with Competition law in the context of data sharing, the Database Directive[33] and the Open Data Directive[34]. Among the most recent texts it takes into considerations also the propositions of the Data Governance Act[35] and it complements the Digital Market Act.[36]

Within this kaleidoscopic set of rules, the Data Act shows a high level of consumer protection, addressing the difficulties that final users usually have in gaining access to information generated by IoT devices; due both to their high technicalities and to a not-always adequate level of consciousness showed by companies. The proposal aims at «further empowering consumers using products or related services to meaningfully control how the data generated by their use of the product or related service is used»[37]. By doing so it imposes a consequent burden on manufacturers as it obliges the data holder to make data available[38] and to transfer them when requested[39] (a sort of "extended right to access" and an "extended right to data portability"). The manufacturers can still access data and use them, but they «would have to design their products in a way that allows the user to access the generated data easily by default and be transparent on what data will be accessible and how to access them»[40]. In the last political agreement, it was better defined the scope of the obligation which will cover intentional and indirect actions and data used and generated in standby mode. As it is still unclear if it will cover organisations based outside the EU, it has been decided that data shall be anonymized and will have to occur in a standardised and real-time manner. [41]

This approach somehow follows the footsteps of the General Data Protection Reg-

[30] European Commission, *Press Release - Data Act.*

[31] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[32] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

[33] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of database.

[34] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.

[35] European Commission, Proposal for a Regulation of the European parliament and of the Council on European data governance (Data Governance Act).

[36] European Commission, Proposal for a Regulation of the European Parliament and the Council on harmonised rules on fair access to and use of data (Data Act).

[37] European Commission, Proposal for Data Act, Explanatory Memorandum, 13.

[38] European Commission, Proposal for Data Act, Chapter III.

[39] European Commission, Proposal for Data Act, Chapter VI.

[40] European Parliamentary Research Service (EPRS), *Briefing – The Data act,* 5 October 2022, available at *europarl.europa.eu*.

[41] L. Bertuzzi, *Data Act: EU institutions finalise agreement on industrial data law*, in *EURACTIV*, 28 June 2023 (updated on 30th June 2023), available at *euractiv.com*.

ulation (for example, by adopting by design and by default principles) and it widens its approach into a more comprehensive requirement of "data management", where data are governed in a user-centric way and therefore explainability, transparency and availability of data must be persistent in every product and service dealing with data.
It shall be noted that the burden imposed on companies might be relieved a little by presuming a compensation for making data available, which shall be «reasonable and agreed with the data recipient».[42] It makes sense as proper and functioning data accesses mechanisms require multi-sector investments in data quality, processes and technical arrangements; as long as data holders may not hinder access to data (or make it too difficult) trying to obtain a remuneration in exchange for information that shall (at least in part) be easily accessible.[43]
Scholars have been given some opinions on the Act, stressing its necessity (and urgency) but also drawing attention to some limits of the proposal. Wolfgang Kerber[44], Professor of Economics at the Marburg University, in Germany, underlines that even though market necessities surrounding the Internet of Things have, indeed, been listed correctly by the Act, there is still a lot of work to do. First, the mechanisms to enforce user right to access still seem to weak to be effective (due to «insufficient scope of data, lacking technical interoperability, high transaction costs, esp. through the need for a negotiated contract with FRAND conditions, unclarity regarding data markets»[45]), second (and extremely relevant for our purposes) the attempt to make user regain control over his/her data «will not work due to unsolved serious market failure problems in B2C situations, i.e. that all the rights to use the IoT data will end up with the data holders (and leave the consumers with only these weak user rights)».[46]
A Data Act is needed, as a huge portion of the market needs regulation, and although it cannot be excluded that some rebalances might be necessary and may be considered in the following steps of the decision process; some adjustments within business processes and consumer-relationships may come in handy to solve (at least partly) some concerns, as it will further be analyzed in the last section of this paper.

2.2. Cybersecurity

The European legislator is investing its resources in enhancing the dedicated cybersecurity landscape, a key component in the development of connected technologies as well as a priority of the Digital Decade, as «cybersecurity is an integral part of Europeans' security. Whether it is connected devices, electricity grids, or banks, aircraft, public administrations, or hospitals they use or frequent, people deserve to do so within the assurance that they will be shielded from cyber threats. The EU's economy,

42 EPRS, *Briefing – The Data act*, p.6(f).

43 J. Drexl, *Data access as a means to promote consumer interests and public welfare – An introduction*, cit., 21.

44 W. Kerber, *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, in *GRUR International*, 2022.

45 Ivi, 1.

46 *Ibidem.*

democracy and society depend more than ever on secure and reliable digital tools and connectivity. Cybersecurity is therefore essential for building a resilient, green, and digital Europe».[47]

Threats to cyber safety are real and increasing: in the tenth edition of the ENISA Threat Landscape (ETL) report[48] among the key trends in cyber threats the Agency affirmed that «DDoS [have been identified for] getting larger and more complex, are moving towards mobile networks and IoT and are being used in the context of cyber-warfare».[49] And «IoT malware has increased over 2021. The change in the first half of 2022 shows the prevalence of IoT targeting malware almost doubling. In the first 6 months of 2022, the attack volume is already higher than had been recorded over the last 4 year»[50].

A multi-front approach[51] has been adopted by European institutions which resulted in a prolific production of cybersecurity provisions devoted to cover specific and diverse aspects of technological security.[52]

In 2013 the Directive on Attacks against Information Systems came into force, aiming at harmonising criminal offences related to information systems. In 2016 the Directive on Security and Information Systems (also known as the NIS Directive) tackled critical infrastructures; replaced on December 2022 by the NIS2 Directive, which broadens the scope the first Directive improving cybersecurity risk management and introducing reporting obligations across strategic sectors (e.g. energy, transport, health and digital infrastructure). Other sectoral legislations adopted are the Directive on the Resilience of Critical Entities (CER) which aims to reduce the cyber vulnerabilities and strengthen the resilience of entities providing essential services that are crucial for the maintenance of vital societal functions, economic activities, public health and safety, and the environment (so-called critical entities);[53] and the DORA Regulation (Regulation on Operational Resilience of the Financial Sector), which "sets uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies)-related services to them, such as cloud platforms or data analytics service."[54]

---

[47] European Commission, *Joint Communication to The European Parliament and the Council on the EU's Cybersecurity Strategy for the Digital Decade.*

[48] As explained in the ENISA website, the ETL is «an annual report on the status of the cybersecurity threat landscape. It identifies the top threats, major trends observed with respect to threats, threat actors and attack techniques, as well as impact and motivation analysis. It also describes relevant mitigation measures».

[49] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape (ETL) Report,* 2022, 11.

[50] Ivi, 50.

[51] P. G. Chiara, *The IoT and the new EU cybersecurity regulatory landscape*, in *International Review of Law, Computers & Technology*, 2022, 118-137.

[52] EPRS, *Briefing EU Legislation in progress "EU cyber-resilience act",* December 2022.

[53] European Commission, *Critical Infrastructure: Commission accelerates work to build up European resilience*, 2022, 18, available at *ec.europa.eu.*

[54] European Council, Press Release: *Digital finance: Council adopts Digital Operational Resilience Act*, 2022, 28, available at *consilium.europa.eu.*

To widen the already broad legal landscape two more instruments have been introduced, specifically designed to assess cybersecurity in relation with connected devices:

- The rsecurity Act, introducing a cybersecurity certification scheme made in Europe.

Such a strong effort on behalf of the European Union is justified as «the absence of a cybersecurity legal framework for product with digital elements incentivises the development of potentially diverging national rules among Member States, threatening an open and competitive single market».[55] A matter that becomes even more urgent with the rising of interoperability protocols which by expanding the possibility of sharing data also increase opportunities for threats and malicious attacks.

2.2.1. The Cyber Resilience Act (CRA)

The proposal, based on the provisions of Article 114 TFUE, is a horizontal piece of legislation with the purpose of harmonizing cybersecurity rules on products with digital elements[56] not covered by any previous regulation, seeking to establish a common ground of cybersecurity rules, ensuring more secure hardware and software products. The CRA imposes a burden on manufacturers who must ensure compliance with European cybersecurity requirements. Products will be subjected to a conformity assessment, and the procedure may vary based on the degree of criticality of the product. The Spanish presidency of the EU Council of Ministers released a fine-tuned version of the text at the beginning of July 2023.[57] The last version of the document obliges manufacturers that become aware of incidents or vulnerabilities to actively inform the competent authority. The task of evaluating the reports has been put in the hands of the national Computer Security Incident Response Teams (CSIRTs) relieving the ENISA from the task which will have to manage a pan-European platform to analyse complementarities and establish a vulnerabilities database.

The proposal used to divide products with digital elements into two categories[58] (as better shown in Figure 1):

- Default non-critical products (like smart home assistants).

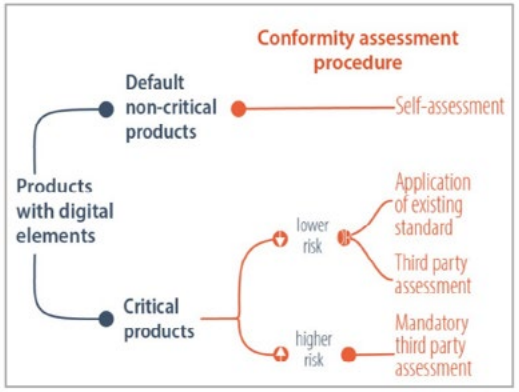

Figure 1. Cyber resilience conformity assessment, Source: EPRS, EU cyber-resilience act – Briefing

[55] EPRS, *Briefing EU Legislation in progress – EU cyber-resilience act*, 2022, 3.

[56] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020* (Cyber Resilience Act).

[57] L. Bertuzzi, *EU ambassadors set to endorse new cybersecurity law for connected devices*, in *EURACTIV*, 2023, available at *euractiv.com*.

[58] EPRS, *Briefing EU Legislation in progress "EU cyber-resilience act"*, 2022, available at *europarl.europa.eu*.

- Critical products, which are further divided into products carrying a higher or lower risk.

However, the last version of the text[59] removed any explicit reference to "highly critical products" and specific assurance level requirements replacing it with a first list of highly critical products categories and the obligation to conduct an impact assessment «to assess the supply and demand side of the internal market and the capability and readiness of the member states for the schemes' implementation»[60] before asking for any mandatory certifications.

Cybersecurity is imperative: the EU is clearly putting an effort to assure that companies and manufacturers are on board with the commitment to ensure a safer experience to their consumers. Therefore, it imposes significant fines on manufacturers who may not follow the given requirements: they might risk 15 million fine or 2.5% of their annual turnover worldwide for non-compliance with the security requirements and/or a 10 million fine or 2% of their total annual turnover worldwide for lack of compliance with all other obligations in the regulation.

The legislative process is still ongoing. The last Swedish presidency of the EU Council suggested three partial compromises to the old text[61] and the Spanish presidency is now working on the text. Among the introductions a couple have an interesting side effect. First, manufacturers must state a potential product lifespan during which customers will receive security updates. Second, it is the economic operators who significantly impact connected devices who are now responsible for adhering to the cybersecurity rules. The introduction of security updates that do not alter a product's intended use actually exempts the creator from this liability. These specifications wave somehow the burden on manufacturers which, righty exists but tries to not exceed the perimeter of doable interventions.

2.2.2. The Cybersecurity Act

The Cybersecurity Act entered into force in June 2019. The document focused on the position of the European Union Agency for Cybersecurity (ENISA) and on the adoption of a European cybersecurity certification.

Thanks to the provisions of the Cybersecurity Act the Agency was granted a permanent mandate and saw an overall enhancement of its role in supporting the Union to achieve a common and high-level cybersecurity. For our purposes, the Act finds its main relevance in the creation of a European cybersecurity certification scheme: a comprehensive set of rules, technical requirements, standards, and procedures agreed at European level for the evaluation of the cybersecurity characteristics of a specific

[59] L. Bertuzzi, *Data Act: EU institutions finalise agreement on industrial data law*, cit.

[60] L. Bertuzzi, *EU ambassadors set to endorse new cybersecurity law for connected devices,* cit.

[61] Among the main suggestions, two further crucial conditions were imposed: first, each linked device needs a special product identifier to enable identification and security patches shall easily identify the applicability of security updates. Second, in order to dispose of a product securely, the text now mandates that the manufacturers provide users with the ability to safely and easily erase all data and settings, including those permitting access to Wi-Fi networks, from the product.

product, service, or process. The project is laudable, and a single certification recognized throughout Europe and validated by a European agency would certainly lend homogeneity to an ever-changing landscape. However, the adoption of the certification scheme is still on a voluntary basis, and this partially nullifies the positives of the initiative. Cybersecurity initiatives, especially in the IoT sector, are definitely supported and promoted at national level (the Finnish Cybersecurity Label proposed by the Finnish Transport and Communications Agency[62] is a perfect example), however a proliferation of certifications may lead to "legal fragmentation in the Single Market"[63] and a common cybersecurity certification scheme (even better if specifically tackling IoT) will definitely help to reach clarity and harmonization.
It shall be noted that the European Union is not the only entity to increase its efforts on preserving the safety of the digital scene. The Organization for Economic Co-operation and Development (OECD) in its Policy Framework on Digital Security published on December 2022 states that «digital security is a means to achieve economic and social objectives rather than an end it itself. Therefore, it is important to design and implement digital security policies that are consistent with those developed in other related policy areas. When designed and/or implemented in isolation, digital security policies are likely to be inconsistent with other policy areas, and to be perceived as burdensome, costly, and counterproductive. When they aim at creating synergies with other policy areas' objectives, digital security policies are likely to be more effective[64]».

2.3. Liability

IoT devices can challenge the traditional notions of civil liability,[65] therefore at the EU level many resources are being invested in assuring that Artificial Intelligence and mechanisms built on AI or integrated with AI systems can be trusted.[66]
When dealing with civil liability the Union does not look at IoT distinctively from AI, but in this context considers AI, IoT and robotics as opportunities to be looked at together, as they all «can combine connectivity, autonomy and data dependency to perform tasks with little or no human control or supervision. […] Their complexity is reflected in both the plurality of economic operators involved […] and the multiplicity of components […]. Added to this is the openness to updates and upgrades after their placement on the market. The vast amount of data involved, the reliance

[62] Finnish Transport and Communications Agency, *Finnish Cybersecurity Label*, 2020, available at: *tietoturvamerkki.fi*.

[63] P.G. Chiara, *The IoT and the new EU cybersecurity regulatory landscape*, in *International Review of Law, Computers & Technology,* 2022, 6.

[64] Organization for Economic Co-operation and Development (OECD), *OECD Policy Framework on Digital Security Cybersecurity for Prosperity*, 2022, 9, available at *oecd.org*.

[65] L. E. Gorman, *The Era of the Internet of Things: Can Product Liability Laws Keep Up?,* in *Defense Counsel Journal*, 84, 2017, 215.

[66] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Building Trust in Human-Centric Artificial Intelligence*, Brussels, 8 April 2019.

on algorithms and the opacity of AI decision-making, make it more difficult to predict the behaviour of an AI-enabled product and to understand the potential causes of a damage. Finally, connectivity and openness can also expose AI and IoT products to cyber-threats».[67]

AI, IoT and robotics represent a chance not to be missed for Europe. In order to maintain a relevant role in the global discussion tables on new technologies, the EU needs not only to make strategic choices (which is one of the main purposes of the Data Act) and impose common technical requirements (plumping up the cybersecurity framework is definitely a step in this direction), but also to hearten its citizens that products and services with digital elements that respond to digital logics are reliable and, whenever necessary, bring with them at least the same remedies as non-digital products. To reduce the degree of uncertainty and to support the commercial objectives underlying the European Digital Decade, the Commission takes into its own hands the task of guaranteeing a high degree of protection to its citizens and it proposes two Directives: the so-called AI Liability Directive[68] and a renewal of the already existing Product Liability Directive.[69]

The Commission assumes a holistic approach: «[t]hese two policy initiatives are closely linked and form a package, as claims falling within their scope deal with different types of liability. The Product Liability Directive covers producer's no-fault liability for defective products, leading to compensation for certain types of damages, mainly suffered by individuals. [The AI Liability Directive] covers national liability claims mainly based on the fault of any person with a view of compensating any type of damage and any type of victim. They complement one another to form an overall effective civil liability system».[70]

2.3.1. AI Liability Directive

Technologies based on AI are intrinsically complex, autonomous, and not always as transparent, therefore users may struggle to understand the underlying logic.[71] Civil liability must ensure victims the opportunity to claim for compensation and a real shot at fair trial,[72] making the claim process accessible. In the eyes of the Union this type

[67] European Commission, Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, *Report on the safety and liability of Artificial Intelligence, the Internet of Things and robotics*, Brussels, 2020, 2.

[68] European Commission, *Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence* (AI Liability Directive).

[69] European Commission, *Proposal for a Directive of the European Parliament and of the Council on liability for defective products.*

[70] European Commission, *Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence* (AI Liability Directive).

[71] They are generally defined "black-boxes", to which are opposed efforts made by scholars and technicians to make the AI "explainable" – on the topic please see: K. K. Chennan et al, *Black Box Model for Explainable Artificial Intelligence*, in M. Metha et al. (eds.), *Explainable AI: Foundations, Methodologies and Applications,* Intelligent Systems Reference Library Volume 232, New York City, 2023, 1 ss.

[72] Art. 47, Charter of Fundamental Rights: «Everyone whose rights and freedoms ranteed

of goal is better addressed at supranational level, in order to avoid rules fragmentation and uncertainty[73] that may come from a merely national approach. The Directive aims at providing a solid basis for compensation to damages caused by AI-systems (eventually in the lack of compliance with national or Union law) and it establishes a "targeted rebuttable presumption of casualty"[74]: a presumption of causal link, which eases the process of causal link identification. This represents a needed support especially in cases where AI are designed as black boxes[75] and are therefore difficult to decipher.
The AI Liability Directive does not directly address Internet of Things products, however, it is relevant for our purposes in that it provides an overall protective framework for the consumer to access remedies and contributes to the creation of a safe and defined legal landscape, positioning itself in accordance with the AI Act, to which it makes repeated references. In fact, even though it cannot used by itself to start a lawsuit under certain conditions can reverse the burden of proof.
The work on the AI Liability Directive is strictly connected to the AI Act, it has been put aside waiting for the final text of the AI Regulation.

2.3.2. Product Liability Directive (PLD)

The proposal for a revision of the Product Liability Directive together with the proposal for the adoption of an AI Liability Directive generate a package of complementary legal instruments, sharing the common goal of adjusting liability to the digital age and AI systems.
The renewal of the Directive takes into consideration a pool of regulations that swings from protection of consumers,[76] to personal data protection, to damages connected with environmental issues. Moreover, references to the Cybersecurity initiatives[77] and other legislative sector-specific[78] rules help assuring a safety framework for products in the EU internal market. Among them, constant referrals to the AI Act (which hopefully will provide some underlying requirements and definitions) promises a general

by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice».

73 Even though the chosen legal instrument to rule on the matter is a "Directive" which leaves some leeway to Member States to implement rules in their own national systems.

74 European Commission, *Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence* (AI Liability Directive), 2022, 13.

75 Please see note 71 for some further references.

76 For example, the Sale of Goods Act and the Digital Content and Service Directive, that deal with consumer protection concerning contractual liability.

77 The Cybersecurity Act and the Cyber-resilience Act, which aim at mitigating cyber-threats while imposing obligations on manufacturers, although they do not specifically address liability.

78 Such as the Machinery Regulation, the proposed General Product Safety Regulation and even the recently adopted Digital Service Act. They do not concern liability issues and responses.

harmonization among the new provisions and it confirms that AI systems and AI-enabled goods indeed fall within the scope of the renewed Directive[79], extending the possibility of compensation also to IoT Products and services, including not only manufacturers of hardware products but also providers of software and digital services.[80] «The PLD proposal will ensure that when AI Systems are defective and cause physical harm, property damage or data loss it is possible to seek compensation from the AI-System provider or from any manufacturer that integrates an AI system into another product».[81] The Directive stipulates that in some specified situations when these are too complicated for the defendant to prove, notably due to technological or scientific complexity, national courts may presume the defectiveness of a product or a causal connection between the damage and the fault. In addition, an economic operator may be exempt from liability if it can show that the defects of the product were not apparent at the time due to the state of science and technology at the time.

At the beginning of March 2023, a draft on the updated Product Liability Directive was presented by Swedish chair of the EU Council. It defines more explicitly the term "manufacturer's control" and aims at reducing national fragmentation on the topic. The text has been updated to reflect a non-paper from the European Commission that made it clear that software, including that offered through "as-a-service" model, like Netflix or Microsoft 365, is a product and therefore is covered by the Act. Similarly, in the March version of the text the associated digital services that are built into or connected to the product have been better defined as, for example, traffic information for a navigation system or a temperature control service that monitors the operation of a smart fridge.[82]

However, one of the last acts of the Swedish presidency, before leaving the chair to the Spanish presidency, was to circulate e new compromise text on the proposal in late May 2023. The last draft law indicates that open software provided for free and outside a commercial activity is excluded from the scope of the liability rules. The text also clarifies that if a manufacturer integrates the open-source software as a component of its product and it consequently causes a defect, the liability will then fall on the

[79] This answers the call for the European Parliament made in 2020: European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence.

[80] Recital 12 of the Product Liability Directive: «Products in the digital age can be tangible or intangible. Software, such as operating systems, firmware, computer programs, applications, or AI systems, is increasingly common on the market and plays an increasingly important role for product safety. Software is capable of being placed on the market as a standalone product and may subsequently be integrated into other products as a component, and is capable of causing damage through its execution. In the interest of legal certainty, it should therefore be clarified that software is a product for the purposes of applying no-fault liability, irrespective of the mode of its supply or usage, and therefore irrespective of whether the software is stored on a device or accessed through cloud technologies. The source code of software, however, is not to be considered as a product for the purposes of this Directive as this is pure information. The developer or producer of software, including AI system providers within the meaning of [Regulation (EU) …/… (AI Act)], should be treated as a manufacturer».

[81] European Commission, Proposal for a Directive of the European Parliament and the Council on liability for defective products, 2022.

[82] L. Bertuzzi, *EU Council refines scope, responsibilities in product liability rulebook*, in *EURACTIV*, 2023, available at *euractiv.com*.

manufacturer rather than the software provider. It is interesting to notice a turnaround compared to March: the EU Council made it clear that internet access services should not be regarded as services products and are therefore not covered by the Directive. In addition, if a product depends on internet connectivity to maintain security and loses connectivity, it will be regarded as defective. This specification is especially crucial for Internet of Things (IoT) products in light of the impending Cyber Resilience Act, which will mandate the enrolment of security fixes over a certain period of time. [83]
Given the history of the PLD, it suffers less its connection with the AI Act: although it exists a Product Liability Directive has been in place since 1985 therefore the work on the document it is sped up compared to the AI Liability Directive. Although there is still space of manoeuvre for change of plans «the co-rapporteurs are pushing on the accelerator to reach a committee-level agreement by September, with bilateral meeting with political groups already kicking off».[84]

2.3.2.1. Circular Economy

The renewed Productive Liability Directive reflects the context of the so-called "circular economy", the EU action plan adopted on March 2020.[85] Generally speaking, a «circular economy is an economic system designed with the intention that maximum use is extracted from resources and minimum waste is generated for disposal».[86] For the business model designed by it, products that are able, through their internet connection, to be modified and/or upgraded to enhance their productivity or to elongate their lifespan are part of the circular economy.[87] In fact, «[i]t is becoming increasingly common for digital services to be integrated in or interconnected with a product in such a way that the absence of the service would prevent the product from performing one of its functions, for example the continuous supply of traffic data in a navigation system. While [The Product Liability] Directive should not apply to services as such, it is necessary to extend no-fault liability to such digital services as they determine the safety of the product just as much as physical or digital components. Such related services should be considered as components of the product to which they are inter-connected, when they are within the control of the manufacturer of that product, in the sense that they are supplied by the manufacturer itself or that the manufacturer

[83] L. Bertuzzi, *EU Council closes in on product liability rulebook,* in *EURACTIV*, 2023, available at *euractiv.com.*

[84] L. Bertuzzi – M. Killeen, *The product liability train, the Commission's AI guidelines*, in *EURACTIV*, 2 June 2023, available at *euractive.com.*

[85] It is one of the main steps of the European Green Deal, for more information please see the dedicated area on the European Commission Website, *Circular economy action plan,* available at *environment.ec.europa.eu.*

[86] P. Deutz, *Circular Economy, International Encyclopedia of Human Geography*, 2020, 193 ss., available at: *sciencedirect.com.*

[87] Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999.

recommends them or otherwise influences their supply by a third party».[88]
However, this also means imposing on manufacturers an obligation to extend their efforts over the products even after the go-to market moment. Indeed, art. 6.1(e) of the revised Directive expands temporally the scope of responsibility of the manufacturer extending it to after the placement of the product on the market. The Article states that:
«1. A product shall be considered defective when it does not provide the safety which the public at large is entitled to expect, taking all circumstances into account, including the following: […]
(e) the moment in time when the product was placed on the market or put into service or, where the manufacturer retains control over the product after that moment, the moment in time when the product left the control of the manufacturer».
According to Article 6 the manufacturer must continue to exercise a certain degree of control over the product even when it is on the market, and it is used by consumers. This control resolves in the obligation to update the product (and its software) and be aware that this operation must be extended to all products able to support it. Furthermore, Recital 37 states that «since digital technologies allow manufacturers to exercise control beyond the moment of placing the product on the market or putting into service, manufacturers should remain liable for defectiveness that comes into being after that moment as a result of software or related services within their control, be it in the form of upgrades or updates or machine-learning algorithms».
These provisions impose on the manufacturer a sort of *de facto* obligation to update or upgrade products, which is particularly relevant when dealing with IoT products that usually undergo a periodical revision process which may easily lead to updates and upgrades.

2.3.2.2. Creating a communication channel with consumers

Usually, consumers are informed of updates as they must take positive actions to physically upgrade the connected appliances. Updates are mainly communicated via push notifications or similar messages, that inform the user that a new version of a software is ready to be installed. The exchange of information results in the creation of a communication channel with the consumer, who gets use to receiving messages from the manufacturer and expects his/her service or product to get better with time (and with the technological advancements). This scenario even creates an expectation in customers to receive communication regarding ameliorations to a certain product or service. At the same time manufacturers have all the interest in users downloading the last version of their technology as through its use they can get feedback and improving their offers even more, better targeting the interest of their consumers. It seems that the PDL (and in some ways even the previous acts analysed) are building the ground for this communication channel to become fundamental, and frequently used.

[88] Product Liability Directive, Recital 15.

A legislative imposition to frequent exchanges with consumers is no news to manufacturers: for example, when dealing with products that consume energy (the so-called energy-using products (EUPs), among which it is also possible to classify Internet of Things) the Ecodesign and Energy Labelling – Framework Directives impose to manufacturers specific[89] and generic requirements[90] which «may entail information requirements, such as material provided by the manufacturer about best practices to use and maintain the product to minimise its environmental impact. [Moreover] it may require that the manufacturer perform a lifecycle analysis of the product to identify alternative design options and solutions for improvement».[91]

Therefore, it seems that manufacturers of energy-consuming products that fall within the scope of the product liability directive shall endeavour to build their communication channel in a transparent manner, structuring the information efficiently enough that it is quickly transposable and suitable for the understanding of end-consumers.

3. Using IoT technology means establishing a relationship with consumers

At the beginning of 2022 the European Commission released a report on a sector inquiry into consumer Internet of Things.[92] The report stated that «in relation to data use cases within consumer IoT companies, respondents [i.e., Businesses involving IoT products and/or services] report that they use the data collected for:

1. the normal functioning of consumer IoT products and services;
2. the personalisation of the user experience;
3. business analytics;
4. product maintenance and development;
5. various other use cases (for example marketing communication, safety and fraud prevention)».[93]

The respondents also pointed out the cost of technology investments and the effort required to be part of the market of the IoT technologies.[94] To be competitive in the IoT sector, technical fundings are accompanied by efforts and investments aimed at preserving data protection rights and answering requests by consumers connected to the use of data. Lately the EU current legislative landscape seems to stress in particular the right to access data and the right to data portability. Especially with the entry onto force of the Data Act these rights will definitely need to be reinforced within

[89] For example, to set limit values to the maximum energy consumption or minimum quantities of recycled material.

[90] For example, that a product is "energy efficient" or "recyclable" (please note that compliance with the relevant harmonised European standard, gives presumption of conformity with the requirement).

[91] European Commission, *Ecodesign your Future – how Ecodesign can help the environment by making products smarter*, 2014, available at *op.europa.eu*.

[92] European Commission, Final Report from the Commission to the Council and the European Parliament, *Final report – sector inquiry into consumer Internet of Things*, 2022.

[93] Ivi, 37.

[94] Ivi, 13.

companies.
It seems that manufacturers of products and services IoT-related are being pushed to put more effort in the way they build and maintain the communication channel with their customers, as the information that are being asked to provide are increasing with the evolving European legal landscape. End-consumers need to be empowered to access their own data (this already as provided by the GDPR and in future also on the basis of the Data Act), to know the security mechanisms related to the connected device they are using (in different ways this is asked both by the GDPR and Cybersecurity initiatives), to receive information about a more energetically conscious use of their products (as requested by the Ecodesign Directives), and to have all the information they need to ask for remedies in case of damages (as stated in the Product Liability Directive).
To further extend the number of information given, along with these requirements also come the protections (and related communications) dictated by provisions on consumer protection.

3.1. Consumer protection

In Spring 2020 the Commission launched the so-called «Fitness Check of EU consumer law on digital fairness [to] determine whether the existing key horizontal consumer law instruments remain adequate for ensuring a high level of consumer protection in the digital environment».[95]
Among other initiatives one that aims at updating consumer protection and keeping it up to date to market requests and changes is the New Deal for Consumers, adopted on April 2022 and as part of the New Deal on 27 November 2019 it was adopted the Directive on better enforcement and modernization of EU consumer protection.[96] The Directive, also known as the "Omnibus Directive" suggested updates to other Directives[97] and while aiming for a general higher degree of transparency in purchases on the digital market (for example asking for clear indications of whether the seller is a professional or not and on who is responsible for deliveries), and for enhanced rights regarding processing of personal data (e.g. right to access and withdrawal period);[98] it also imposed an obligation to inform consumers «about how offers are ranked in search results and identify paid advertisements»[99] and about price changes on specific

[95] European Commission, *Review of EU consumer law*, available at *commission.europa.eu*.

[96] Member States were called to transpose the new rules in their systems by the end of November 2021 and rules should have become effective by May 2022. However, not all Member States have done the necessary activities yet.

[97] Directives involved are: The Unfair Commercial Practices Directive (2005/29/EC); The Unfair Contract Terms Directive (93/13/EEC); The Consumer Rights Directive (2011/83/EU); The Price Indications Directive (98/6/EC).

[98] Other provisions refer to ensuring that price reduction claims are genuine, that remedies against harm are effective or that reviews can be certified.

[99] European Commission, Factsheet, *New Consumer rights – what benefits will I get?*, 2022, available at *commission.europa.eu*.

offers, so «that they are aware of the risk that the asking price was increased».[100]
The Omnibus Directive seems to be fitted to be part of the general approach suggesting more attentive, transparent, and frequent conversations with consumers, who shall be constantly informed of changes and given the necessary instruments to understand the internal market and its movements.

4. Conclusions: marketing communications and legal information may share some purposes

Attempting at drawing together the provisions analysed, a few considerations can be made.
First, entering the IoT market as a responsible manufacturer requires investments on multi and different levels and many proposed legislations will force companies to allocate resources on different areas of their businesses to legally and safely produce and market IoT devices and/or IoT-related services.
Second, the provisions analysed set out a general imposition (or at least a strong suggestion) to communicate with customers in an understandable and consistent way, which (again) requires studies, investments, resources and attention to create products and services that are transparent and explicable by design but also to build a structure able to answer the requests of consumers.
Third, usually there are limitations to the time a business can use data related to its customers for commercial purposes (for example for marketing activities or campaigns). Entities are requested to ask for consent and when the time validity of the given consent has expired communications shall stop and data must be erased. A specific opinion of the Italian Data Protection Supervisory Authority states that: «[a]t all events, the detailed data on the items purchased by identifiable customers may be retained for profiling or marketing purposes for no longer than twelve or twenty-four months, respectively, as of their storage, subject to their being actually anonymised in such a way as to prevent data subjects from being identified also indirectly and/or via interconnections with other databases». Some exceptions have been suggested by the same Authority when dealing with luxury goods[101], although underlying that for other type of products the limit of the validity of consent for marketing purposes is 24 months.[102]
Manufacturers will be torn between information that are or will be obliged to give (in-

[100] *Ibidem.*

[101] Garante Privacy, "*Fidelity card" e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione*, 24 febbraio 2005 (doc. web 1103045).

[102] Relevant provisions on the matter, all by the Italian Data Protection Supervisory Authority are: Garante Privacy, *Verifica preliminare. Prolungamento dei tempi di conservazione dei dati personali riferiti alla clientela per il loro utilizzo a fini di profilazione e di promozione commerciale profilata*, 18 aprile 2018 (doc. web 8997404); Garante Privacy, *Verifica preliminare. Trattamento di dati personali riferiti alla clientela per finalità di profilazione e promozionale*, 5 luglio 2017 (doc. web 6844421); Garante Privacy, *Trattamento e conservazione di dati personali della clientela per finalità di profilazione. Verifica preliminare richiesta da Bulgari S.p.A.,* 24 aprile 2013 (doc. web 2499354).

formation contained in the privacy policy, changes in the processing of data,[103] ways to make your device more energetically efficient, safety measures…etc) and information that they economically benefit form, like communications related to marketing actions and campaigns. Moreover, even though not all information requires to the same economical investments, if the sanctions usually implied to lack of compliant with the EU provisions and/or the loss of profits when marketing communications are shut down are to be considered, the commercial and economic implications related to the establishment and management of a communication channel with consumers are relevant.
Fourth, as many studies showed[104] consumers are not very keen to be slowed down by communications given by providers or manufacturers and their attention to additional information are limited to a short time frame.
Fifth, as said, connected devices (such as smart home appliances) use and generate a huge quantity of data, both personal and non-personal, a characteristic that is intrinsic in the nature of the IoT technology. Data generated and collected create patterns based on the everyday life of consumers. This strong connection with habits of consumers is what makes a service or a product efficient, but it also makes it dependent to a continuous flow of data, which must be governed in a responsible way by data holders.
From these observations, it seems that when it comes to IoT-related products and services, there are different types of information that overlap with each other but have one final recipient: the consumer.
Manufacturers are required to disentangle different standards, keeping in mind that communications must be simple, effective, reliable and, for them to also be economically feasible, as standard as possible. Therefore, a responsible attitude in this regard could be precisely to create a single communication channel, which may have different layers of security and types of information given, segmented and composable, and which allows to prolong a type of communication that is clear and does not confuse the user.
It may be based on a granular and transparent consent, easier to govern and compliant with different security standards based on the different kind of data processed. It can be administered in the same moment as the privacy policy, to avoid imposing a further burden on consumers. Moreover, structures already in use to address privacy-related rights can be leveraged both in terms of data access and in managing consumer requests. The channel can be created with a major effort on explainability and may use design support such as Legal-Design. Establishing one communication channel may get the user used to receive communication on actions he/she may autonomously perform to enhance the use of its device and/or its security, allowing upgrades to be perceived sooner and easier as insert in a trustworthy relationship between the man-

[103] Article 29 Data Protection Working Party, Article 29 Working Party Guidelines on transparency under Regulation 2016/679, 2018, 16, available at: ec.europa.eu/newsroom/article29/items/622227.

[104] A. M. McDonald – L. F. Cranor, *The Cost of Reading Privacy Policies*, in *A Journal of Law and Policy for the Information Society*, 4, 2008, 543 ss.; P. G. Inglesant - M. A. Sasse, *The true cost of Unusable Password Policies: Password Use in the wild*, SIGCHI - Conference on Human Factors in Computing Systems, New York, 2010; B. Anderson - A. V., Brock Kirwan - D. Eargle - Seth Howard, *Users aren't (necessarily) lazy: Using NeuroIS to explain habituation to security warnings*, in *International Conference on Information Systems*, 2014.

ufacturer and the consumer. Moreover, these users that have huge benefit from using IoT technologies but also must rely on them more frequent (for example disabled people) more and cleared information on the type of data manufacturer are collecting will be available, hopefully accompanied by efficient mechanisms to change preferences and settings.

Data-Oriented Strategies:

1) *Minimize:* The amount of processed personal data should be restricted to the minimal amount possible.
2) *Hide:* Any personal data, and their interrelationships, should be hidden from plain view.
3) *Separate:* Personal data should be processed in a distributed fashion, in separate compartments whenever possible.
4) *Aggregate:* Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.

Process-Oriented Strategies:

1) *Inform:* Data subjects should be adequately informed whenever personal data is processed.
2) *Control:* Data subjects should be provided agency over the processing of their personal data.
3) *Enforce:* A privacy policy compatible with legal requirements should be in place and should be enforced.
4) *Demonstrate:* Be able to demonstrate compliance with the privacy policy and any applicable legal requirements.

Figure 2. Privacy and Design strategies of J.-H. Hoepman, Source: C. Li and B. Palanisamy, Privacy in Internet of Things: From Principles to Technologies," in *IEEE Internet of Things Journal*

This type of solution can itself be structured in a segmented manner, exploiting principles of "privacy by design". Among the strategies that may better match the analysis produced so far, one wants to be highlighted. A strategy proposed by Hoepman[105] and taken up by Li and Palanisamy [106] in their paper, consisting of eight "data-oriented" and four "process-oriented" strategies, as better illustrated in Figure 2 below.[107] The presence of process-oriented strategies fit well into business contexts and design strategies have been proved to improve the perception of consumer and the understandability of information given to them.[108]

Finally, this structure is built to respect the very nature of Internet of Things as «several existing IoT systems are designed using a layered architecture. In an IoT system, data is usually collected by end devices, transmitted through communication networks, processed by local/remote servers and finally provided to various applications. Thus, […] data as it flows through multiple layers of the architecture stack, needs […] protection at all layers. Here, implementing proper [data] design strategies based on the roles of the layers in the lifecycle of the data is important. Otherwise, techniques implemented at a specific layer may become either insufficient ([for example legal requirements are] breached at other layers) or redundant ([data] has been protected by techniques implemented at other layers)».[109] The said approach can also be a starting point for manufacturers that can work in a compliant environment from the very first moment

[105] J. H. Hoepman, *Privacy Design Strategies*, in *Information and Communication Technology*, in N. Cuppens-Boulahia – F. Cuppens – S. Jajodia – A. Abou El Kalam – T. Sans (eds.), *ICT Systems Security and Privacy Protection*, SEC 2014. IFIP Advances in Information and Communication Technology, vol 428, Berlin - Heidelberg, 2014, 446 ss.

[106] C. Li – B. Palanisamy, *Privacy in Internet of Things: From Principles to Technologies*, in *IEEE Internet of Things Journal,* 2019, 488 ss.

[107] A graphic summary of the strategies highlighted by Hoepman can be found in the work of C. Li and B. Palanisamy, *Privacy in Internet of Things: From Principles to Technologies*, in *IEEE Internet of Things Journal*, 2019, 488 ss.

[108] Many studies were conducted on the topic by Professor Cranor, among others: L. F. Cranor, *Necessary but not sufficient: standardized mechanisms for privacy notice and choice*, in *Journal on Telecoomunication & High Technology Law,* 10, 2012, 273 ss.

[109] C. Li - B. Palanisamy, *Privacy in Internet of Things: From Principles to Technologies,* cit.

a new technology is thought and created. This can even enhance the interoperability among smart devices, facilitating even more conversations with consumers and save time and energy.[110]

The purpose of this work was to highlight how IoT asks for a multidisciplinary approach[111] to be regulated. Internet of Things and its implications with the life of consumers must be looked at from a legislative point of view, but to better govern its implications business strategies (meaning with it communication plans, economical tactics and process considerations) must also be considered and this will mainly show in the relationships with final costumers. Efforts from different areas and sectors are required and end-users shall not only be involved but products and services must be designed as user-centric. To reach such level of involvement context shall be dynamic and integrated, «given the pervasive, distributed and dynamic nature of IoT»[112] where high-level information is provided to consumers in a trustworthy form and in a transparent environment. This can result in scenarios where platforms are studied in a user-centric way and where accessibility and accountability become a recognisable distinctive element, capable of becoming a reputational benefit for business and entities.

[110] A. Saeed et al., *Energy Efficient Hybrid IoT System for Ambient Living,* Switzerland, 2022.

[111] A. Skarmeta et al., *User-Centric Privacy*, in S. Ziegler (ed.), *Internet of Things Security and Data Protection*, Cham, 2019, 9 ss.

[112] Ivi, 200.

Note a sentenza

Data economy: la Corte di giustizia precisa il rapporto tra concorrenza e protezione dei dati personali e le norme sulla pubblicità personalizzata

Guido d'Ippolito

Corte di giustizia, 4 luglio 2023, C-252/21, *Meta c. Bundeskartellamt*

Un'autorità garante della concorrenza di uno Stato membro può constatare, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa, ai sensi dell'art. 102 TFUE, che le condizioni generali d'uso di tale impresa relative al trattamento dei dati personali e la loro applicazione non sono conformi al regolamento (UE) 2016/679, qualora tale constatazione sia necessaria per accertare l'esistenza di un tale abuso. Alla luce dell'obbligo di leale cooperazione, l'autorità nazionale garante della concorrenza non può discostarsi da una decisione dell'autorità nazionale di controllo competente o dell'autorità di controllo capofila competente che riguardi tali condizioni generali o condizioni generali analoghe. Laddove nutra dubbi sulla portata di tale decisione, o dette condizioni siano, al contempo, oggetto di esame da parte di tali autorità, o, ancora in assenza di un'indagine o di una decisione di dette autorità, ritenga che le condizioni in questione non siano conformi al regolamento (UE) 2016/679, l'autorità nazionale garante della concorrenza deve consultare dette autorità di controllo. In assenza di obiezioni o di risposta di queste ultime entro un termine ragionevole, l'autorità nazionale garante della concorrenza può proseguire la propria indagine.

Il trattamento di dati personali effettuato da un operatore di un social network online può essere considerato necessario per l'esecuzione di un contratto del quale gli interessati sono parti solo a condizione che detto trattamento sia oggettivamente indispensabile per realizzare una finalità che costituisce parte integrante della prestazione contrattuale destinata a quegli stessi utenti, cosicché l'oggetto principale del contratto non potrebbe essere conseguito in assenza di tale trattamento.

Il trattamento di dati personali effettuato da un operatore di un social network online può essere considerato necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi solo a condizione che il suddetto operatore abbia indicato agli utenti presso i quali i dati sono stati raccolti un legittimo interesse perse-

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

guito dal loro trattamento, che tale trattamento sia effettuato entro i limiti di quanto strettamente necessario alla realizzazione di tale legittimo interesse e che dal contemperamento dei contrapposti interessi, alla luce di tutte le circostanze pertinenti, risulti che le libertà e i diritti fondamentali e gli interessi di tali utenti non prevalgono su detto legittimo interesse del titolare del trattamento o di terzi.
La circostanza che l'operatore di un social network online occupi una posizione dominante sul mercato dei social network online non osta, di per sé, a che gli utenti di tale social network possano validamente acconsentire al trattamento dei loro dati personali effettuato da tale operatore. Tale circostanza costituisce nondimeno un elemento importante per determinare se il consenso sia stato effettivamente prestato validamente e, in particolare, liberamente, circostanza che spetta a detto operatore dimostrare.

Sommario

Keywords

abuso di posizione dominante - contratto e consenso - pubblicità personalizzata - autorità indipendenti - data economy.

1. Introduzione

La regolazione delle piattaforme digitali e della c.d. "*data economy*" è un aspetto centrale di quello che è stato definito "costituzionalismo digitale"[1]. L'enorme disponibilità di informazioni, la loro facile reperibilità sulle piattaforme di intrattenimento e *social networking*, insieme allo sviluppo tecnologico che ha trasformato gli algoritmi in complessi "sistemi di intelligenza artificiale", ha permesso la nascita di modelli di business fondati sulla remunerazione dell'attenzione e del tempo "speso" dagli utenti sulle piattaforme digitali; piattaforme divenute sempre più potenti e titolari di un'influenza non solo economica ma quasi "sociale"[2].

[1] Per una disamina sugli autori e le teorie alla base del concetto di costituzionalismo digitale si veda O. Pollicino, *Potere digitale* (voce), in *Enciclopedia del diritto*, Milano, V, 2023, 410 ss.

[2] P. Stanzione (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, 2022; L. Bolognini (a cura di), *Privacy e libero mercato digitale. Convergenza tra regolazioni e tutele individuali nell'economia data-driven*, Milano, 2021; E. Cremona, *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Napoli, 2023; Con riferimento ai rapporti "*Platform-to-Business*" quale particolare forma di asimmetria nei rapporti tra imprese, si veda F. Ruggeri, *Poteri privati e mercati digitali. Modalità di esercizio e strumenti di controllo*, Roma, 2023, disponibile in *open access* sul sito dell'editore; S. Martinelli, *I contratti nella platform economy. Ruoli e responsabilità delle piattaforme*, Torino, 2023; A. Iannotti della Valle, *Le regole di Internet tra poteri pubblici e privati. Tutela dei diritti e ruolo dell'antitrust in una prospettiva costituzionale*, Napoli, 2023.

In quelli che sono stati definiti "mercati dell'attenzione"[3] la risorsa principale e contesa dai fornitori di servizi digitali sono le informazioni e i dati personali degli utenti; il modo per ottenerli è catturare la loro attenzione: più questi sono attratti dai servizi offerti più resteranno sulla piattaforma e più l'interazione con quest'ultima produrrà informazioni di rilievo commerciale come i gusti, gli interessi, le abitudini, la capacità di spesa o gli orientamenti di consumo dell'utente nel tempo, ecc. Il rovescio della medaglia di questo sistema è, come rilevato in letteratura[4], un sistema basato sul tracciamento e monitoraggio continuo dell'attività degli utenti su larga scala.

Quest'incetta di dati e informazioni è alla base dei principali modelli di business nei mercati digitali. Dal punto di vista giuridico ciò conduce ad almeno due temi: quello ancora tutt'altro che risolto della monetizzazione e commercializzazione dei dati personali[5]; quello della regolazione della pubblicità online (*display advertising*), in particolare nella sua forma automatizzata e basata su profilazione degli utenti, ossia la pubblicità personalizzata, profilata o, anche, "targettizzata"[6].

Tali temi sono oggetto di esame da parte del legislatore europeo, nell'ambito della corposa regolazione sulla "*European Strategy for data*", e sempre più al centro di pronunce dalle autorità giurisdizionali e amministrative dei vari Stati membri.

In tale contesto si inserisce la Corte di giustizia dell'UE con la sentenza del 4 luglio 2023.

Quest'ultima acquisisce importanza non solo per le tematiche di particolare attualità e rilievo sulle quali la Corte è stata chiamata a pronunciarsi, ma anche per lo straordinario raggio di azione della sua analisi.

A partire dal rapporto tra la normativa in materia di protezione dei dati personali e quella a tutela della concorrenza, la Corte esamina le norme del regolamento (UE) 2016/679 (in seguito, anche, "Regolamento" o "GDPR") fornendo indicazioni alcune delle quali costituenti l'esito e il riconoscimento di riflessioni già avviate, altre invece, risultano più innovative e si pongono come preziosa regolamentazione del settore.

[3] Y.N. Harari, *21 lezioni per il XXI secolo*, Milano, 2018, 116.

[4] Sebbene la letteratura e i report, anche di istituzioni e autorità di controllo, sul tema siano sempre più abbondanti, basti qui richiamare S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019. La stessa Corte di giustizia in commento sembrerebbe riprendere tale concetto al punto 118 laddove afferma che trattamenti particolarmente "estesi" hanno un notevole impatto sull'utente tanto da «suscitare in quest'ultimo la sensazione di una continua sorveglianza della sua vita privata».

[5] Tra la sempre più corposa dottrina: E. Cremona–F. Laviola–V. Pagnanelli (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Torino, 2022; V. Ricciuto, *Circolazione e scambio dei dati personali. Il problema della regolazione del nuovo fenomeno patrimoniale*, in *Rivista di diritto dell'impresa*, 2, 2021, 261 ss.; Id., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, e A. De Franceschi, *Il "pagamento" mediante dati personali*, entrambi in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 23 ss. e 1389 ss.; G. Malgieri-B. Custers, *Pricing privacy: the right to know the value of your personal data*, in *Computer Law & Security Review*, 2017.

[6] Per una generale analisi del trattamento di profilazione e la disciplina della pubblicità personalizzata online sia consentito rinviare a: G. d'Ippolito, *Profilazione e pubblicità targettizzata online. Real-Time Bidding e behavioural advertising*, Napoli, 2021.

2. Il fatto

Con sentenza del 4 luglio 2023 la Corte di giustizia si occupa della competenza di un'autorità nazionale per la concorrenza ad esaminare i comportamenti di un'impresa alla luce di talune disposizioni del Regolamento, soffermandosi anche sull'applicazione di alcuni istituti: come il rapporto tra il contratto e il consenso quale base giuridica di alcuni trattamenti.

Il caso origina dall'istruttoria dell'autorità federale tedesca garante della concorrenza (Bundeskartellamt) che ha portato al divieto per Meta di trattare taluni dati personali sulla base delle condizioni generali di utilizzo del social network Facebook.

In particolare, l'oggetto della contestazione del Bundeskartellamt è la raccolta e il trattamento dei dati esterni alla piattaforma, i dati cc.dd. "Off Facebook": derivanti dalla consultazione di pagine Internet e applicazioni di terzi collegate al servizio Facebook o riguardanti l'utilizzo degli altri servizi appartenenti al gruppo Meta come Instagram, WhatsApp o Oculus.

Per la raccolta e il trattamento dei dati Off Facebook Meta utilizzava quale base giuridica il contratto *ex* art. 6, par. 1, lett. b), del Regolamento.

Poiché Meta considerava il trattamento di tali dati come necessario al servizio (Facebook) offerto all'utente ne disciplinava la raccolta e l'utilizzo all'interno delle sue condizioni contrattuali[7]. Essendo questo un documento che l'utente può solo accettare o rifiutare, secondo il noto approccio "*take it or leave it*", la conseguenza pratica è che il trattamento di dati ulteriori a quelli prodotti dalla piattaforma Facebook è sottratto ad una specifica valutazione e autorizzazione dell'utente. Semplificando, per il trattamento di questi dati non è richiesto un autonomo consenso agli utenti/interessati del trattamento[8].

Il Bundeskartellamnt, nel ritenere il trattamento dei dati Off Facebook non conforme al GDPR, ha concluso che ciò costituisse uno sfruttamento abusivo della posizione dominante di Meta sul mercato dei sociali network online.

Sicché, con decisione del 6 febbraio 2019, ha vietato a Meta di subordinare l'uso del social network Facebook, tramite condizioni generali di contratto, al trattamento dei dati Off Facebook e di procedere, senza il consenso degli utenti, al trattamento di tali dati. Inoltre, ha ordinato di adeguare le condizioni generali in modo che risultasse chiaramente che tali dati non sarebbero stati né raccolti, né messi in relazione con gli account degli utenti Facebook, né utilizzati senza il consenso dell'utente, chiarendo che tale consenso non è valido se inteso come una condizione per l'utilizzo del social

[7] Sui presupposti per il ricorso al contratto come fondamento di liceità del trattamento si vedano le linee guida del Comitato europeo per la protezione dei dati personali: EDPB, *Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati*, versione 2.0, 8 ottobre 2019.

[8] Può essere utile rilevate che tale costruzione è sostanzialmente analoga a quella eseguita, sempre da Meta, con riferimento alla pubblicità personalizzata, in particolare nella sua forma più invasiva di pubblicità comportamentale (*behavioural advertising*). Anche in questo caso Meta inseriva il trattamento di profilazione degli utenti per finalità pubblicitarie nelle sue condizioni contrattuali senza richiedere un autonomo consenso agli interessati e, anche in tale caso, è stata contestato a Meta il ricorso alla base giuridica contrattuale. La vicenda si è conclusa con la decisione sanzionatoria del 31 dicembre 2022 della Data Protection Commission irlandese.

network.
Avverso tale decisione, l'11 febbraio 2019 Meta presentava ricorso dinanzi all'Oberlandesgericht Düsseldorf (Tribunale superiore del Land di Düsseldorf). Successivamente apportava modifiche alle proprie condizioni generali: indicando espressamente che l'utente, invece di pagare per l'uso dei prodotti Facebook, acconsente alle inserzioni pubblicitarie[9]; introducendo la possibilità per gli utenti Facebook di visualizzare un riepilogo delle informazioni che le società del gruppo Meta ottengono in relazione alle loro attività su altri siti Internet e applicazioni e di scollegare tali dati dal loro account Facebook.com, sia per il passato che per il futuro.
L'Oberlandesgericht Düsseldorf, nel nutrire dubbi sulla possibilità per le autorità per la concorrenza di controllare, nell'ambito dell'esercizio delle loro competenze, la conformità di un trattamento di dati personali alle condizioni stabilite nel GDPR, sospendeva il procedimento per sottoporre alla Corte alcune questioni pregiudiziali.
Innanzitutto si chiede alla Corte di esprimersi sulla possibilità di un'autorità per la concorrenza di uno Stato membro di constatare, nell'ambito dell'esame di un abuso di posizione dominante ai sensi dell'art. 102 TFUE, che le condizioni contrattuali operate da tale impresa siano conformi al Regolamento e, eventualmente, accertarne la violazione e disporne la fine. In aggiunta, si chiede alla Corte l'interpretazione di alcune norme del Regolamento.

3. Le considerazioni della Corte

La Corte di giustizia chiarisce innanzitutto che: «Il modello economico del social network online Facebook si fonda sul finanziamento tramite la pubblicità online, che viene creata su misura per i singoli utenti del social network in funzione, in particolare, del loro comportamento di consumo, dei loro interessi, del loro potere d'acquisto e della loro situazione personale. Il presupposto tecnico per questo tipo di pubblicità è la creazione automatizzata di profili dettagliati degli utenti del network e dei servizi online offerti a livello del gruppo Meta. A tal fine, oltre ai dati che gli utenti forniscono direttamente al momento della loro iscrizione ai servizi online di cui trattasi, vengono raccolti, all'interno e all'esterno di detto social network e dei servizi online forniti dal

[9] Tale diversa strategia comunicativa implica un primo ancorché ancora ambiguo riconoscimento del fenomeno della commercializzazione dei dati personali non solo in senso astratto ma anche con specifico riferimento alla piattaforma Facebook che, fino a quel momento, quanto meno nelle aule di tribunale per fini difensivi, aveva sostenuto l'impossibilità di scambiare servizi contro dati personali. A tal riguardo si veda la vicenda giudiziaria che ha visto lo scontro tra Facebook e l'Autorità Garante della Concorrenza e del Mercato che, con provvedimento n. 27432, procedimento PS11112, del 29 novembre 2018, ha contestato a Facebook una pratica commerciale ingannevole per aver pubblicizzato come "gratuito" l'accesso al proprio servizio mentre questo era remunerato tramite il trattamento dei dati degli utenti. Tale ricostruzione è stata confermata dapprima dal Tar Lazio, Sez. I, 10 gennaio 2020, n. 260, e poi dal Consiglio di Stato, sez. VI, 29 marzo 2021, n. 2631.
Il riconoscimento della fornitura "gratuita" del servizio digitale in cambio dell'ostensione di inserzioni pubblicitarie sta inoltre apparendo nelle informative di altri servizi digitali come, per esempio, TikTok, dove nei suoi Terms of Service, al §4, si legge: «*We don't charge you a fee to use most of the features of the Platform. Instead, businesses and organisations pay us to show you ads for their products and services, and we may also charge sellers a commission on products sold on TikTok Shop*».

gruppo Meta e messi in relazione ai loro diversi account di utenza, anche altri dati relativi a tali utenti e ai loro dispositivi. Il quadro generale di tali dati consente di trarre conclusioni dettagliate sulle preferenze e sugli interessi dei medesimi utenti»[10].
La Corte riassume il principale modello di business delle piattaforme digitali, quello definito "*zero-price*", nel quale viene offerto un servizio in cambio non di un corrispettivo monetario bensì dell'autorizzazione dell'utente al trattamento dei propri dati per finalità commerciali (c.d. "patrimonializzazione"[11] o "valorizzazione" dei dati personali): dalla vendita delle informazioni o dei *pattern* statistici, ossia gli schemi di consumo degli utenti, all'invio di messaggi pubblicitari personalizzati, ecc.[12].

3.1. Sulla valutazione incidentale del GDPR da parte di un'autorità per la concorrenza

Sebbene le norme del Regolamento non si rivolgano alle autorità nazionali per la concorrenza ma disciplinino la cooperazione tra le autorità nazionali di controllo (in materia di protezione dei dati personali) interessate e l'autorità di controllo capofila nonché, se del caso, la cooperazione con il Comitato europeo per la protezione dei dati (EDPB), nonché il fatto che le autorità di controllo e le autorità per la concorrenza perseguano obiettivi e compiti propri, la Corte osserva che l'accesso e lo sfruttamento dei dati personali è di fondamentale importanza per l'economia digitale.
Questo conduce a ritenere il trattamento dei dati personali un parametro significativo della concorrenza. Escludere le norme in materia di protezione dei dati personali dall'analisi concorrenziale significherebbe ignorare la realtà di tale evoluzione economica e pregiudicare l'effettività della concorrenza nell'Unione Europea.
Sicché conclude la Corte: «nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa su un dato mercato, può risultare necessario che l'autorità garante della concorrenza dello Stato membro interessato esamini anche la conformità del comportamento di tale impresa a norme diverse da quelle rientranti nel diritto della concorrenza, quali le norme in materia di protezione dei dati personali previste dal GDPR»[13].
La Corte specifica che l'esame del GDPR è un accertamento incidentale nell'ambito della constatazione di un abuso di posizione dominante e che l'autorità per la concorrenza non si sostituisce all'autorità di controllo. Non è compito dell'autorità per la concorrenza sindacare il rispetto del Regolamento né far uso dei poteri riservati alle

[10] CGUE, C-252/21, *Meta c. Bundeskartellamt* (2023), § 27. I modelli di business basati sulla raccolta e riutilizzo dei dati personali per fini commerciali e, più specificatamente, per finalità di pubblicità personalizzata, sono ormai noti alla giurisprudenza, come Consiglio di Stato n. 2631 del 29 marzo 2021, ma anche l'Autorità Garante della Concorrenza e del Mercato. Si vedano a tal riguardo, oltre a quelli altrove citati, anche i provvedimenti del 9 novembre 2021, n. 29888, PS11150, contro Apple (iCloud) e del 16 novembre 2021, n. 29890, PS11147, contro Google Drive-Sweep.

[11] TAR Lazio, sez. I, 10 gennaio 2020, n. 260.

[12] Sui modelli di business si veda M. Mursia–C.A. Trovato, *The commodification of our digital identity: limits on monetizing personal data in the European context*, in questa *Rivista*, 3, 2021, 165 ss.

[13] CGUE, C-252/21, cit., § 48.

autorità di controllo.
Da ciò ne segue che anche l'autorità per la concorrenza sarà soggetta all'interpretazione che le autorità di controllo o la stessa Corte danno al Regolamento e a questa dovrà conformarsi, pur restando libera di trarne le proprie conclusioni sotto il profilo dell'applicazione del diritto alla concorrenza. Nei casi dubbi o sui quali non è rinvenibile un precedente, l'autorità per la concorrenza e quella di controllo dovranno cooperare tra loro.
Tale cooperazione si sostanzia nel fatto che, qualora l'autorità per la concorrenza abbia necessità di esaminare la conformità di un'attività al Regolamento e tale attività non sia già stata oggetto di una decisione da parte dell'autorità di controllo o della Corte e ciononostante ritenga che tale attività non sia conforme alle disposizioni del Regolamento, oppure quando nutra dubbi sulla valutazione effettuata dall'autorità di controllo o un'attività simile sia, al contempo, oggetto di esame da parte di tali autorità, in tutti questi casi l'autorità per la concorrenza dovrà consultare l'autorità di controllo al fine di fugare i propri dubbi o determinare se attendere l'adozione di una decisione da parte quest'ultima prima di iniziare la propria valutazione[14].
Dall'altra parte, l'autorità di controllo deve rispondere alla richiesta di cooperazione entro un termine ragionevole comunicando le informazioni di cui dispone e che possano consentire di fugare i dubbi o, se del caso, informando dell'intenzione di avviare il procedimento di cooperazione di cui agli artt. 60 e seguenti del Regolamento[15].
La Corte crea così un'ipotesi di parere obbligatorio per i casi dubbi o nuovi, vincolante con riferimento all'interpretazione del GDPR ma non con riferimento agli accertamenti di natura concorrenziale, bilanciato da un meccanismo di silenzio assenso. Infatti, in assenza di risposta dell'autorità di controllo o nel caso in cui questa non sollevi obiezioni a che si prosegua senza una sua decisione, l'autorità per la concorrenza potrà proseguire la propria indagine[16].
La ricostruzione di tale meccanismo si basa più su un riconoscimento pratico delle difficoltà sottese agli accertamenti istruttori delle autorità che sulla forma giuridica e, tanto più, tale approccio risulta condivisibile nella misura in cui mira a garantire una tutela effettiva all'utente. Rafforzando la collaborazione tra autorità si dà così attuazione al principio di leale cooperazione sancito all'articolo 4, par. 3, TUE che si affianca, così, alla giurisprudenza che regola i rapporti tra normativa consumeristica e sul corretto trattamento dei dati personali[17].
Recentemente il Consiglio di Stato[18] ha ricostruito il rapporto tra la normativa a tutela del consumatore e quella sul corretto trattamento di dati personali non in termini di "compartimenti stagni di tutela" bensì come "tutela multilivello" suscettibile di

[14] Ivi, § 57.

[15] Ivi, § 58.

[16] *Ibid.*

[17] Con riferimento alla disciplina consumeristica si veda la Corte di giustizia del 13 settembre 2018, nelle cause riunite C-54/17 e C-55/17, ECLI:EU:C:2018:710, che ha avuto origine e impatti nella giurisprudenza nazionale alla quale si farà cenno nel prosieguo con riguardo all'art. 27, c. 1-*bis*, d.lgs. 206/2005.

[18] Cons. Stato, sez. VI, 29 marzo 2021, n. 2631.

amplificare la garanzia dei diritti delle persone. In altre parole, la disciplina sul corretto trattamento dei dati personali e quella del Codice del consumo (d.lgs. 206/2005) presentano ambiti operativi differenti ma non contrastanti. Non si rinviene «alcuna incompatibilità o antinomia tra le previsioni del "Regolamento privacy" e quelle in materia di protezione del consumatore, in quanto le stesse si pongono in termini di complementarietà, imponendo, in relazione ai rispettivi fini di tutela, obblighi informativi specifici, in un caso funzionali alla protezione del dato personale, inteso quale diritto fondamentale della personalità, e nell'altro alla corretta informazione da fornire al consumatore al fine di fargli assumere una scelta economica consapevole»[19].

La cooperazione descritta dalla Corte acquisisce, inoltre, particolare importanza laddove, non solo l'Autorità Garante della Concorrenza e del Mercato (AGCM)[20] sembra già porre alla base delle sue valutazioni in tema di concorrenza il rispetto del GDPR – da ultimo nell'importante caso relativo all'ipotesi di abuso di posizione dominante da parte di Google per aver ostacolato l'esercizio del diritto alla portabilità dei dati *ex* art. 20 GDPR[21] – ma soprattutto perché questo principio sembrerebbe già rintracciabile, sebbene con riferimento alle pratiche commerciali scorrette, nell'art. 27, c. 1-*bis*, d.lgs. 206/2005[22].

La norma dispone che nei casi di pratiche commerciali scorrette integrate da comportamenti regolati da specifiche normative europee, l'AGCM conserva la sua competenza ad intervenire a condizione che richieda il parere della "Autorità di regolazione competente" in quel settore.

La sua applicazione era stata rivendicata dal Garante per la protezione dei dati personali (in seguito, anche, "Garante" o "GPDP") all'esito del provvedimento con il quale l'AGCM aveva sanzionato Telepass per una pratica commerciale ingannevole nell'attività di distribuzione di polizze assicurative. La contestazione della pratica ingannevole derivava dall'aver accertato che le società del gruppo Telepass non avevano adeguatamente informato gli utenti che i loro dati sarebbero stati condivisi con compagnie e intermediari di assicurazione o comunque raccolti e utilizzati anche a fini commerciali[23].

In sede di ricorso al TAR il Garante si era costituito contestano il difetto di istruttoria e la violazione delle regole del procedimento poiché l'AGCM non aveva richiesto il suo parere come prescritto dalla norma citata.

Il TAR Lazio rigetta tale motivo ritenendo non applicabile la norma in quanto il Garante non sarebbe una "autorità regolatoria di settore" ma una "autorità generalista preposta alla tutela trasversale di un diritto fondamentale". Inoltre, sostiene il giudice amministrativo, i piani tra tutela del consumatore e corretto trattamento dei dati

[19] TAR Lazio, sez. I, 10 gennaio 2020, n. 260, § 8.

[20] Oltre all'autorità tedesca, che ha portato la questione dinanzi la Corte di giustizia, e all'AGCM, si rileva anche l'attività dell'Autorité de la concurrence francese che, a luglio 2023, ha avviato un'istruttoria per abuso di posizione dominante contro Apple per condizioni discriminatorie, non obiettive e non trasparenti sull'utilizzo dei dati degli utenti a fini pubblicitari. Il comunicato stampa del 25 luglio 2023 è disponibile sul sito dell'autorità.

[21] AGCM, provvedimento 18 luglio 2023, n. 30736, procedimento A552.

[22] M. Cappai, *Quando l'erosione dei limiti costituzionali avviene dall'interno: il caso dell'art. 27, comma 1-bis del codice del consumo e della sua (presunta) natura interpretativa*, in *Rivista AIC*, 2, 2018, 1 ss.

[23] AGCM, provvedimento del 9 marzo 2021, n. 28601, procedimento PS11710.

personali sono "autonomi" e nulla in più avrebbe aggiunto il parere del Garante sul provvedimento finale[24].
Quand'anche tale pronuncia possa essere considerata conforme alla giurisprudenza previgente[25], spicca il differente approccio del TAR rispetto a quello della Corte dinanzi una questione analoga. Mentre la Corte di giustizia è andata al cuore del problema, il TAR ha fatto perno su una logica giuridica che ci restituisce però una tutela formale e probabilmente non più al passo coi tempi.
Al contrario, proprio un approccio più concreto e il focus sul principio di leale cooperazione tra autorità amministrative nonché il meccanismo di consultazione introdotto dalla Corte di giustizia potrebbero consentire un'interpretazione estensiva della norma tale da considerare anche il Garante quale autorità preposta all'applicazione di una normativa europea e, quindi, quale "autorità regolatoria" di un certo "settore"[26]. Ciò, ovviamente, non al fine di contestare l'ormai pacifica competenza dell'AGCM in materia di pratiche commerciali scorrette bensì di fornire alla stessa, in ottica di leale cooperazione, appunto, ulteriori e utili elementi di valutazione per la sua attività di tutela del mercato e dei consumatori.
L'auspicio è quindi che la cooperazione tra AGCM e Garante possa rafforzarsi e indirizzarsi verso i binari di un confronto stabile a tutto vantaggio della tutela di un soggetto che, a prescindere dalla specifica nomenclatura di settore, consumatore o interessato del trattamento, nel contesto digitale coincide sostanzialmente con la persona[27].

3.2. Sull'applicazione delle norme del GDPR

Successivamente la Corte si sofferma sull'analisi degli altri quesiti prospettati dal giudice del rinvio e riguardanti pratiche diffuse tra i fornitori di servizi digitali.
Con riferimento alle categorie particolari di dati personali *ex* art. 9 del Regolamento, la Corte afferma che, ferma la necessità di un accertamento in concreto, in generale nel caso in cui un utente di un social network consulti siti Internet oppure applicazioni correlate a una o più delle categorie particolari di dati, il trattamento di tali dati da parte dell'operatore del social network – consistente nel raccogliere dati risultanti dalla con-

[24] TAR Lazio, sez. I, 9 novembre 2022, n. 603.

[25] Per una disamina sulla giurisprudenza in materia di conflitti di attribuzione tra le diverse autorità, in particolare tra AGCM e autorità di settore, ivi compresa la già citata Corte di giustizia 13 settembre 2018, nonché il passaggio dall'art. 23, c. 12-*quinquiesdecies,* del decreto legge n. 95 del 2012 al c. 1-*bis*, dell'art. 27, d.lgs. 206/2005, si veda M. Cappai, *La repressione delle pratiche commerciali scorrette nei mercati regolati: cosa aspettarsi dalla Corte di giustizia?*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 3-4, 2017, 879 ss.

[26] A tal fine può essere utile rilevare che la posizione rivendicata dal Garante può essere sovrapposta a quella che, a suo tempo, l'Adunanza Plenaria del Consiglio di Stato ha attribuito all'Autorità per le Garanzie nelle Comunicazioni (AgCom) in casi analoghi a quello Telepass: anche nei casi Vodafone e Wind le pratiche commerciali considerate dall'AGCM scorrette erano state realizzate tramite la violazione di obblighi informativi oggetto di una disciplina speciale, quella afferente al settore delle comunicazioni elettroniche di competenza dell'AgCom, così come nel caso Telepass gli obblighi informativi afferiscono al settore della protezione dei dati personali di competenza del Garante. Cfr. Cons. Stato, Adunanza Plenaria, nn. 3 e 4 del 2016.

[27] Anche qui si veda Cons. Stato, sez. VI, 29 marzo 2021, n. 2631.

sultazione di tali siti e applicazioni nonché i dati inseriti dall'utente, oppure nel mettere in relazione l'insieme di tali dati con l'account del social network di quest'ultimo – deve essere considerato un trattamento di categorie particolari di dati lecito solo nel rispetto dell'art. 9 del Regolamento[28].

L'art. 9, par. 2, lett. e), del Regolamento consente il trattamento di questi dati se l'interessato li ha resi "manifestamente pubblici". Rileva però la Corte che questo avviene soltanto se l'interessato abbia espresso chiaramente la sua volontà in tal senso, sulla base di un'impostazione individuale di parametri effettuata con piena cognizione di causa, o se vi abbia esplicitamente acconsentito sulla base di un'informazione espressa fornita dal sito o applicazione prima di tale inserimento o attivazione[29].

Sicché quando un utente consulta siti Internet oppure applicazioni correlate ad una o più delle categorie particolari di dati ed inserisce tali dati o attiva pulsanti come «Mi piace» o «Condividi» o i pulsanti che consentono all'utente di identificarsi utilizzando il proprio account, numero di telefono o indirizzo di posta elettronica, dati poi raccolti e utilizzati dall'operatore di social network mediante cookie o altri marcatori, l'utente non rende manifestamente pubblici tali dati solo per queste attività. I dati potranno essere considerati resi manifestamente pubblici soltanto se l'utente abbia esplicitamente e preventivamente acconsentito a far ciò, oppure tale intenzione la si può desumere dall'aver l'utente impostato, tramite gli strumenti messi a disposizione dalla piattaforma e, come sottolinea la Corte, "con piena cognizione di causa", la sua interazione con la piattaforma in modo da rendere i suoi dati pubblicamente accessibili a un numero illimitato di persone[30].

Sebbene le osservazioni riguardino specificamente le categorie particolari di dati personali, la Corte sembra applicare il principio generale per cui i dati non possono essere né raccolti né trattati né riutilizzati[31] in assenza di una giustificazione legalmente riconosciuta[32]. Ciò vale, sia per i dati comuni che per le categorie particolari di dati che, come osserva la Corte, possono essere trattati solo sulla base dei fondamenti di liceità dell'art. 9 GDPR.

Secondo la Corte, se il sito o l'applicazione utilizzata è idonea a rivelare la presenza di categorie particolari di dati allora il trattamento riguarderà categorie particolari di dati e non dati comuni, con le restrizioni e maggiori garanzie dell'art. 9 GDPR rispetto all'art. 6.

---

[28] CGUE, C-252/21, cit., § 73.

[29] Ivi, §§ 82-83.

[30] Ivi, §§ 84-85.

[31] Le condizioni e i presupposti per il "riutilizzo" dei dati sono contenuti in diversi atti normativi tra cui i recenti Data Governance Act e Data Act. Ciononostante, il principio base sembrerebbe rinvenirsi nel principio di "limitazione delle finalità del trattamento", di cui all'art. 5, par. 1, lett. b), GDPR, per il quale i dati personali possono essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità». Sul tema sia consentito rinviare a G. d'Ippolito, *Il principio di limitazione delle finalità del trattamento tra data protection e antitrust. Il caso dell'uso secondario di big data*, in *Il diritto dell'informazione e dell'informatica*, 6, 2018, 943 ss.

[32] Tale principio è declinato nelle varie norme del GDPR ma ha le sue radici già nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea che, al par. 2, recita: «[I dati di carattere personale] devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge».

Si tratta dell'affermazione di un principio che potrebbe avere criticità applicative non sempre prevedibili tant'è che la Corte ne subordina l'applicazione a una valutazione caso per caso; infatti: «spetterà al giudice del rinvio stabilire se i dati in tal modo raccolti […] consentano effettivamente di rivelare informazioni di questo tipo»[33].

Inoltre, la Corte rileva che per "riutilizzare" dati presenti o ottenibili in qualunque modo online (*rectius*, per trattare i dati disponibili online per fini diversi o ulteriori rispetto a quelli per cui sono stati originariamente resi disponibili) non si può invocare la base giuridica di cui all'art. 9, par. 2, lett. e), del Regolamento perché i dati semplicemente disponili online non sono per ciò solo "manifestamente pubblici" in assenza di un elemento volitivo in più: la prova che l'utente voglia effettivamente rendere pubblicamente disponibili i suoi dati.

Si sconfessa così la diffusa quanto erronea credenza che tutto ciò che è online, per il fatto solo di essere disponibile, sia anche riutilizzabile. Ciò vale per le opere dell'ingegno così come per i dati personali quali ulteriori beni immateriali. Ma, soprattutto, tale specificazione sembra colpire tutte quelle attività che, senza idonea base giuridica, raccolgono i dati prodotti dall'interazione con la piattaforma o tramite c.d. "*scraping*", una sorta di pesca a strascico di dati disponibili online[34], da riutilizzare per diversi fini: dall'*enrichment* delle proprie banche dati, al *training* degli algoritmi, attività strategica specie per i recentemente noti sistemi di Intelligenza Artificiale generativa[35].

3.3. Sul contratto e il consenso come base giuridica di alcuni trattamenti tra cui la pubblicità personalizzata

Dopodiché la Corte si sofferma sui presupposti di due tra i più discussi e controversi fondamenti di liceità previsti dall'art. 6 del Regolamento: il contratto e il legittimo interesse.

Possono i c.d. dati "Off Facebook" – ossia provenienti da altri servizi, diversi da quello principale, o derivanti dalla consultazione di altri siti o applicazioni di terzi – essere messi in relazione o "incrociati" con i dati del social network sulla base della necessità di eseguire il contratto con gli utenti, oppure per il perseguimento del legittimo interesse del titolare o di terzi?

---

[33] CGUE, C-252/21, cit., § 72.

[34] Nel provvedimento del 10 febbraio 2022, n. 50, doc. web n. 9751362, contro Clearview AI, il Garante per la protezione dei dati personali rilevava che: «Quanto, in particolare al *data scraping*, trattasi di una modalità particolare di raccolta che avviene a completa insaputa degli interessati. Sulla scorta di quanto sopra, si può ragionevolmente concludere che la raccolta di dati personali liberamente disponibili in Internet mediante tecniche di *web scraping* costituisce un trattamento di dati personali, che deve trovare legittimazione in una delle basi giuridiche previste dall'art. 6 del Regolamento». Con riferimento alla costituzione di elenchi telefonici a partire da numeri disponibili online si veda GPDP, Provvedimento del 17 maggio 2023, n. 201, doc. web n. 9903067.

[35] Tra le contestazioni mosse dal Garante per la protezione dei dati personali alla società OpenAI e che ha portato alla limitazione provvisoria del trattamento dei dati degli utenti italiani tramite ChatGPT si rinviene «l'assenza di idonea base giuridica in relazione alla raccolta dei dati personali e al loro trattamento per scopo di addestramento degli algoritmi sottesi al funzionamento di ChatGPT». GPDP, provvedimento 30 marzo 2023, n. 112, doc. web n. 9870832.

La Corte rileva innanzitutto che affinché un trattamento di dati personali sia considerato necessario all'esecuzione di un contratto di cui all'art. 6, par. 1, lett. b), del Regolamento, esso deve essere oggettivamente indispensabile per realizzare una finalità che è parte integrante della prestazione contrattuale destinata all'interessato. Bisogna quindi dimostrare in che modo l'oggetto principale del contratto non potrebbe essere conseguito in assenza del trattamento che si intende operare; non basta che il trattamento sia semplicemente "utile", semplifichi o in altro modo agevoli l'esecuzione della prestazione principale offerta all'utente ma il trattamento deve essere "essenziale" per la corretta esecuzione del contratto stipulato con l'interessato[36].

È, questa, un'interpretazione rigorosa del concetto di "necessità"[37] che giustifica il ricorso al contratto ma in linea con una giurisprudenza[38] che, dopo la Corte di giustizia, è difficile non considerare "consolidata" se non "granitica".

Per quanto riguarda il legittimo interesse, la stessa giurisprudenza della Corte[39] ha individuato le condizioni che devono cumulative ricorrere per il suo utilizzo: il perseguimento di un interesse considerato "legittimo"; la "necessità" del trattamento per la realizzazione del legittimo interesse perseguito; la condizione che gli interessi o i diritti e le libertà fondamentali dell'interessato alla tutela dei dati non prevalgano sul legittimo interesse del titolare del trattamento o di terzi (c.d. *balancing test*)[40].

Ciò premesso la Corte conclude che la personalizzazione dei contenuti, ancorché utile per l'utente[41], non appare necessaria per offrire a tale utente i servizi del social network online.

Allo stesso modo, per utilizzare Facebook non è necessario iscriversi agli altri servizi del gruppo Meta e il trattamento di dati provenienti da servizi diversi da quello principale non sembra essere necessario per consentire la fornitura di quest'ultimo servizio[42].

Con riferimento al legittimo interesse, la Corte esamina alcuni trattamenti.

Per svolgere attività di pubblicità personalizzata sulla base del legittimo interesse bisogna tenere in considerazione alcuni elementi come la necessità del trattamento, la minore età dell'interessato o le aspettative degli utenti. Proprio in considerazione di tali

[36] CGUE, C-252/21, cit., §§ 97 ss.

[37] CGUE, C-524/06, *Heinz Huber c. Bundesrepublik Deutschland* (2008), ECLI:EU:C:2008:724.

[38] CGUE, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke e Eifert* (2010), EU:C:2010:662; Si veda, inoltre, EDPB, *Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento*, cit., § 25 ss. e, da ultimo, la vicenda giudiziale che ha visto contrapposto la DPC contro Meta con riferimento all'utilizzo del contratto quale base giuridica della pubblicità comportamentale: EDPB, *Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)*, 5 December 2022; e, conseguentemente, DPC, *Decision concerning a complaint directed against Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) in respect of the Facebook Service decision*, 31st day of December 2022.

[39] CGUE, C-13/16, *Rigas satiksme* (2017), EU:C:2017:336, §§ 28 ss.; C-597/19, *M.I.C.M.* (2021), EU:C:2021:492.

[40] Sui presupposti del legittimo interesse si veda anche: WP29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, 9 aprile 2014, 41 ss.

[41] Non mancano studi di carattere economico che rilevano come la personalizzazione dei contenuti esponga al rischio di messaggi pubblicitari di prodotti di qualità media a prezzi superiori: E.A. Schnadower Mustri–I. Adjerid–A. Acquisti, *Behavioral advertising and consumer welfare: an empirical investigation*, Federal Trade Commission PrivacyCon 2022.

[42] CGUE, C-252/21, *Meta c. Bundeskartellamt*, §§ 102 ss.

aspettative la Corte afferma che: «malgrado la gratuità dei servizi di un social network online quale Facebook, l'utente di quest'ultimo non può ragionevolmente attendersi che, senza il suo consenso, l'operatore di tale social network tratti i suoi dati personali a fini di personalizzazione della pubblicità. In tali circostanze, si deve ritenere che i diritti fondamentali e gli interessi di tale utente prevalgano sull'interesse dell'operatore a tale personalizzazione della pubblicità mediante la quale egli finanzia la sua attività, cosicché il trattamento da quest'ultimo effettuato a tali fini non può rientrare nell'ambito di applicazione dell'articolo 6, paragrafo 1, primo comma, lettera f), del GDPR»[43].

È questo uno dei passaggi della sentenza su cui più si è soffermata l'attenzione di giornalisti, studiosi ed esperti in quanto regolamenta uno dei trattamenti principali per il modello di business delle piattaforme digitali: quello della pubblicità personalizzata online.

Già le autorità di controllo, con propri provvedimenti[44] o linee guida dell'EDPB[45], avevano sostanzialmente ricondotto la pubblicità personalizza al consenso quale base giuridica. Il mercato era poi stato "scosso" dalla pronuncia dell'autorità di controllo irlandese (DPC) che, su parere vincolante dell'EDPB, aveva precluso il ricorso al contratto quale base giuridica[46].

La sentenza della Corte di giustizia, anch'essa suscettibile di avere effetti e ripercussioni ben più ampi del singolo caso da cui ha avuto origine, completa l'opera precludendo anche il ricorso al legittimo interesse[47] e, di fatto, riportando la scelta sull'unica base giuridica allo stato utilizzabile: il consenso.

Proprio tale sentenza è divenuta l'occasione per l'autorità di controllo norvegese di vietare a Meta di svolgere trattamenti di pubblicità comportamentale sulla base del legittimo interesse[48], base giuridica a cui la società americana aveva fatto ricorso proprio a causa della "bocciatura" dello strumento negoziale da parte della DPC.

Che il consenso sia, nei fatti, la base giuridica allo stato ritenuta adeguata per la pubblicità comportamentale sembrerebbe, infine, essere riconosciuto anche dalla stessa Meta che, dopo l'intervento dell'autorità norvegese, ha annunciato di abbandonare ogni proposito di ricorso al legittimo interesse per adottare il consenso[49]. Ciò quantomeno per

---

[43] Ivi, § 117.

[44] Oltre ai provvedimenti già citati si vedano, con specifico riferimento al consenso, anche: CNIL, *Délibération de la formation restreinte n° SAN-2023-009 du 15 juin 2023 concernant la société Criteo*; CNIL, *Délibération SAN-2019-001 du 21 janvier 2019 concernant Google*; in generale, con riferimento all'utilizzo di cookie e marcatori, la normativa impone il ricorso al consenso (in Italia l'art. 122 d.lgs. 196/2003). Obbligo normativo ripreso dalle linee guida delle diverse autorità di controllo nazionali.

[45] Oltre alle linee guida sul contratto, si vedano: WP29, *Parere 2/2010 sulla pubblicità comportamentale online*, 22 giugno 2010; EDBP, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 4 maggio 2020; EDPB, *Linee guida 8/2020 sul targeting degli utenti di social media*, Versione 2.0, 13 aprile 2021.

[46] EDPB, *Binding Decision 3/2022, cit.*; DPC, *Decision concerning a complaint directed against Meta, cit.*

[47] In tal senso si era espresso anche il Garante per la protezione dei dati personali che con provvedimento del 7 luglio 2022, n. 248, doc. web n. 9788429, avvertiva TikTok che il proposito di fondare la pubblicità personalizzata sulla base del legittimo interesse avrebbe potuto configurare una violazione della normativa.

[48] Datatilsynet, *Urgent and Provisional Measures – Meta*, 21/03530-16, 14.07.2023. Disponibile anche il comunicato stampa sul sito dell'autorità.

[49] Meta, *How Meta Uses Legal Bases for Processing Ads in the EU*, January 4, 2023 update on August 01,

il mercato dell'UE, dello Spazio Economico Europeo e della Svizzera, Regno Unito escluso[50]. Potrebbe questo essere l'epilogo di una battaglia legale durata anni e che Meta ha condotto non solo per sé ma a difesa di un intero modello di business largamente adoperato.

Con questa sentenza della Corte, i fornitori di servizi digitali si trovano per la seconda volta in meno di un anno[51], solo per l'imitarsi al settore della pubblicità online, dinanzi la scelta di proseguire come prima o rinnovarsi e ripensare il mercato con modelli di business più sostenibili.

Dopo la pubblicità personalizzata, l'esame della Corte si volge verso altri trattamenti.

Con riferimento alla sicurezza del network, che ben può, astrattamente, configurare un legittimo interesse del titolare, per utilizzare tale base giuridica bisognerà in concreto verificare che tale obiettivo non possa ragionevolmente essere raggiunto in modo altrettanto efficace ma con mezzi meno pregiudizievoli e nel rispetto del principio della minimizzazione dei dati. Nello specifico, con riferimento alla fattispecie portata dal giudice del rinvio, bisognerà verificare se e in quale misura il trattamento di dati personali raccolti a partire da fonti esterne al social network Facebook risulti effettivamente necessario per garantire che non sia compromessa la sicurezza interna di tale network[52].

Con riferimento ai trattamenti diretti al "miglioramento del prodotto o servizio", per quanto anche questo astrattamente in grado di integrare un interesse del titolare meritevole di tutela, la Corte avanza dubbi che possa prevalere sui diritti fondamentali e sugli interessi degli utenti, tanto più se minorenni[53].

Relativamente al trattamento riguardante l'informazione delle autorità preposte all'esercizio di azioni penali e all'esecuzione di pene dirette ad evitare, individuare e a perseguire reati, tale obiettivo non può, in linea di principio, costituire un legittimo interesse ai sensi dell'art. 6, par. 1, lett. f), del GDPR[54].

Infine, con riferimento ai dati "Off Facebook" la Corte conclude che tale trattamento: possa essere considerato necessario per l'esecuzione di un contratto solo a condizione

---

2023: «*Today, we are announcing our intention to change the legal basis that we use to process certain data for behavioural advertising for people in the EU, EEA and Switzerland from 'Legitimate Interests' to 'Consent'. This change is to address a number of evolving and emerging regulatory requirements in the region, notably how our lead data protection regulator in the EU, the Irish Data Protection Commission (DPC), is now interpreting GDPR in light of recent legal rulings, as well as anticipating the entry into force of the Digital Markets Act (DMA). Historically, businesses operating in this region have relied on a variety of legal bases under GDPR for the purpose of processing data for advertising. GDPR states that there is no hierarchy between legal bases, and none should be considered more valid than any other. However, we have listened carefully to regulatory feedback from the Irish DPC, including how it is interpreting recent decisions by the European Court of Justice, in deciding to make this change*».

[50] Si veda, a riguardo, la dichiarazione del 2 agosto 2023 di Stephen Almond, Executive Director of Regulatory Risk dell'Autorità di controllo inglese (ICO): «*We're aware of Meta's plans to seek consent from users for behavioural advertising in the EU, to the exclusion of the UK. This follows related findings by the Court of Justice of the European Union, Irish Data Protection Commission and Norwegian Data Protection Authority. We are assessing what this means for information rights of people in the UK and considering an appropriate response*».

[51] Tre se si conta anche l'importante pronuncia dell'autorità belga del febbraio 2022 contro IAB Europe e il sistema pubblicitario basato sul protocollo TCF: BE DPA, *Complaint relating to Transparency & Consent Framework. Decision on the merits 21/2022*, 2 February 2022.

[52] CGUE, C-252/21, cit., §§ 19 ss.

[53] Ivi, § 123.

[54] Ivi, § 124.

che sia oggettivamente indispensabile per realizzare una finalità che costituisce parte integrante della prestazione contrattuale destinata agli utenti, cosicché l'oggetto principale del contratto non potrebbe essere conseguito in assenza di tale trattamento[55], cosa che non si realizza nel caso concreto[56]; mentre può essere considerato necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi solo a condizione che si informino gli utenti che tale trattamento sia effettuato entro i limiti di quanto strettamente necessario e che dal contemperamento dei contrapposti interessi, alla luce di tutte le circostanze pertinenti, risulti che le libertà e i diritti fondamentali e gli interessi di tali utenti non prevalgono su detto legittimo interesse[57].

Infine, con riguardo alla possibilità di trattare i dati Off Facebook per la salvaguardia di interessi vitali (art. 6, par. 1, lett. d), Regolamento) o per adempiere a un obbligo legale (art. 6, par. 1, lett. c), Regolamento), la Corte rileva, rispettivamente, che: un operatore, la cui attività riveste carattere essenzialmente economico e commerciale, non può addurre la protezione di un interesse essenziale alla vita dei suoi utenti o di un'altra persona per giustificare la liceità di tale trattamento[58]; mentre tale trattamento potrà avvenire allorché sia effettivamente necessario per adempiere un obbligo legale rispondente ad un obiettivo di interesse pubblico e a questo proporzionato nei limiti dello stretto necessario[59].

3.4. Sul rapporto tra posizione di dominanza e validità del consenso

Una ulteriore e rilevante questione sottoposta alla Corte si incentra sulla possibilità di considerare valido, ai sensi del Regolamento, il consenso prestato dall'utente nei confronti di un operatore in posizione dominante in un certo mercato.

La Corte premette una serie di rilievi. Innanzitutto, il consenso non può essere considerato liberamente prestato se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio, oppure quando esiste un evidente squilibrio tra l'interessato e il titolare del trattamento[60].

In aggiunta si sofferma su una norma che ha creato non poche questioni applicative[61]: l'art. 7, par. 4, del Regolamento che prevede che, nel valutare se il consenso sia stato

[55] Ivi, §125.

[56] Ivi, § 104: «Pertanto, e salvo verifica del giudice del rinvio, un trattamento di dati personali provenienti da servizi diversi da quello del social network online, proposti dal gruppo Meta, non sembra essere necessario per consentire la fornitura di quest'ultimo servizio».

[57] Ivi, § 126.

[58] Ivi, § 137.

[59] Ivi, § 138.

[60] EDBP, *Linee guida 5/2020 sul consenso*, cit., § 13 ss. Si veda anche il considerando 43 del GDPR.

[61] G. Resta-V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile*, 2, 2018, 411 ss.; S. Thobani, *Operazioni di "tying" e libertà del consenso*, in *Giurisprudenza italiana*, 3, 2019, 533 ss. Si veda anche, con riferimento alla "fungibilità" dei trattamenti, Cass. civ., sez. I, 25 luglio 2018, n. 17278.

liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto[62].

È la norma che disciplina il c.d. *tying* o *bundling*, di grande attualità specie con riferimento alla questione dei *cookie wall* e *pay wall* implementati da diversi editori online: ossia condizionare la prestazione di un servizio al conferimento del consenso a un trattamento di dati a questo non necessario. Principio che, nel caso dei *cookie wall*, si è tradotto nella scelta, rimessa all'utente, tra consentire la profilazione tramite cookie per accedere al sito oppure pagare una certa somma di denaro.

La liceità di tale condotta è stata oggetto di interpretazione restrittiva da parte dell'EDPB[63] così come dall'Autorità di controllo francese (CNIL). Quest'ultima, in seguito all'intervento del Conseil d'Etat[64], è ritornata sui propri passi per disciplinare i casi di condizionalità lecita[65].

La questione è, inoltre, attualmente *sub iudice* dinanzi il Garante italiano[66].

Su tali temi la Corte conclude che, certamente, anche l'operatore titolare del trattamento che occupi una posizione dominante sul mercato dei social network può ricorrere al consenso come base giuridica ma, allo stesso tempo, tale circostanza deve essere presa in considerazione nella valutazione della validità del consenso in quanto può incidere sulla libertà di scelta dall'utente. L'utente potrebbe quindi non essere in grado di rifiutare o di revocare il consenso senza subire pregiudizio[67]. Proprio l'esistenza di una posizione dominante è suscettibile di creare uno squilibrio evidente tra l'interessato e il titolare che può favorire l'imposizione di condizioni non strettamente necessarie all'esecuzione del contratto.

La Corte di giustizia afferma quindi che: «tali utenti devono disporre della libertà di rifiutare individualmente, nell'ambito della procedura contrattuale, di prestare il loro

---

[62] La seconda frase del considerando 43 del GDPR precisa che si presume che il consenso non sia stato liberamente espresso, dove l'uso dell'espressione «si presume», così come interpretato dall'EDPB nelle linee guida sul consenso (v. punto 35 di dette linee guida) indica che i casi di validità del consenso saranno estremamente eccezionali. *Cfr.* EDBP, *Linee guida 5/2020 sul consenso*, *cit.*, punto 14, dove si rileva che l'inciso «tra le altre» indica che l'art. 7, par. 4, GDPR non è stato redatto in modo esaustivo e può comprendere altre eventualità, compresa qualsiasi azione di pressione o influenza inappropriata sull'interessato, che impedisca a quest'ultimo di esercitare il suo libero arbitrio, § 25 ess e, in particolare, il § 26 dove si rileva che il GDPR assicura che il trattamento dei dati personali per cui viene richiesto il consenso non possa trasformarsi direttamente o indirettamente in una controprestazione contrattuale e, quindi, che le due basi legittime per la liceità del trattamento, il consenso e l'esecuzione di un contratto, non possono essere riunite e rese indistinte.

[63] EDBP, *Linee guida 5/2020 sul consenso*, *cit.*, punto 39 dove si legge: «Affinché il consenso sia prestato liberamente, l'accesso ai servizi e alle funzionalità non deve essere subordinato al consenso dell'utente alla memorizzazione di informazioni o all'ottenimento dell'accesso a informazioni già memorizzate nell'apparecchiatura terminale dell'utente (i cosiddetti "cookie wall")».

[64] Conseil d'État, Décision du 19 juin 2020; si veda anche CNIL, *Cookies et autres traceurs: le Conseil d'État rend sa décision sur les lignes directrices de la CNIL*, 19 juin 2020.

[65] CNIL, *Cookie walls: la CNIL publie des premiers critères d'évaluation*, 16 mai 2022.

[66] GPDP, *Cookie wall: all'esame del Garante privacy le iniziative degli editori*, 18 ottobre 2022, doc. web n. 9815415.

[67] CGUE, C-252/21, §§ 148-149.

consenso a operazioni particolari di trattamento di dati non necessarie all'esecuzione del contratto, senza essere per questo tenuti a rinunciare integralmente alla fruizione del servizio offerto dall'operatore del social network online, il che implica che a detti utenti venga proposta, se del caso a fronte di un adeguato corrispettivo, un'alternativa equivalente non accompagnata da simili operazioni di trattamento di dati»[68].

È quindi opportuno che possa essere prestato un consenso separato per il trattamento dei dati Off Facebook. Diversamente, anche in considerazione della posizione dominante[69] di Meta e fermo restando che grava sul titolare l'onere di dimostrare che l'interessato ha validamente prestato il proprio consenso, si deve presumere[70] che il consenso di detti utenti al trattamento dei dati Off Facebook non sia stato prestato liberamente.

In conclusione, l'eventuale posizione dominante dell'operatore integra gli elementi di valutazione alla base dell'applicazione dell'art. 7, par. 4, del Regolamento. Circostanza che può essere particolarmente utile in alcuni casi, non ultimo quello dei *cookie wall* posti in essere dagli editori online.

Se pure la Corte fornisce alle autorità di controllo un elemento di valutazione in più, incentrato sulla posizione di dominanza dell'operatore, non si risolve comunque l'interpretazione del vero punto dolente: quando un servizio alternativo possa dirsi "equivalente" a quello condizionato e quindi quando questo possa rendere lecito il sempre più diffuso fenomeno della condizionalità[71].

Ad ogni modo, mentre in apertura si riconosceva alle autorità per la concorrenza la possibilità di accertare, *incidenter tantum*, le norme del Regolamento, qui la Corte sembrerebbe riconoscere anche alle autorità di controllo di fare lo stesso con la normativa sulla concorrenza, consentendogli di porre, alla base delle loro valutazioni sulla validità del consenso, anche l'analisi sulla dominanza del titolare in un certo mercato.

4. Conclusioni

Nell'avallare le tesi del Bundeskartellamt la Corte di giustizia ha emesso una sentenza che avrà importanti ripercussioni su tutto il settore della *data economy*. Ne risulta inoltre rafforzata quella corrente di pensiero che vede in una maggior trasversalità applicativa delle normative la chiave per garantire alla persona nel mondo dei bit una tutela completa ed effettiva.

Si possono poi individuare alcune tendenze in materia di pubblicità personalizzata e regolazione delle piattaforme.

Con riferimento alla base giuridica della pubblicità personalizzata, dopo report del

[68] Ivi, § 150.

[69] Nelle sue conclusioni, l'Avvocato Generale Athanasios Rantos, al § 75, specificava che: «Occorre, tuttavia, precisare, da un lato, che, affinché una situazione siffatta di potere sul mercato sia rilevante sotto il profilo dell'applicazione del GDPR, essa non deve necessariamente essere equiparata al livello di posizione dominante ai sensi dell'articolo 102 TFUE e, dall'altro, che tale circostanza non può da sola, in linea di principio, privare di qualsiasi validità un consenso».

[70] Considerando 43 GDPR.

[71] EDPB, *Linee guida 5/2020 sul consenso*, cit., § 37; CNIL, *Cookie walls*, cit.

Parlamento europeo[72], diverse pronunce delle autorità di controllo[73], linee guida e interventi dell'EDPB[74], e, ora, la sentenza della Corte di giustizia, è difficile continuare a sostenere che gli attuali modelli di business, spesso basati su *dark pattern*[75] e un ridotto potere di controllo degli interessati sui propri dati, possano continuare a prevedere una profilazione degli utenti per fini pubblicitari o commerciali su una base giuridica diversa dal consenso.

Per quanto lecite e condivisibili le istanze del mercato sulla necessità di remunerare la loro attività tramite la profilazione degli utenti si può osservare che la normativa, così come l'interpretazione della stessa, non mira a limitare l'attività d'impresa o lo sviluppo economico, cosa che sarebbe in contrasto, tra le varie norme, anche con l'art. 1 dello stesso Regolamento[76], bensì a tener conto anche della volontà degli utenti nel trattamento dei loro dati. Se, dunque, quella di offrire servizi "a prezzo zero" è una libera scelta di mercato diretta ad abilitare la forma più remunerativa ma anche invasiva di pubblicità personalizzata (la pubblicità comportamentale[77]), dall'altro lato non lo si potrà fare contro la volontà dell'utente, condizionando o forzando la stessa o a sua insaputa.

In altre parole, qualora si scelga di svolgere un trattamento particolarmente impattante sulla sfera giuridica dell'interessato si dovrà contestualmente assumere il rischio che l'utente possa non essere d'accordo. Rischio in realtà condiviso anche dall'utente vista la facilità con cui si ottiene il consenso tutt'altro che consapevole dello stesso, cosa che ha messo in crisi i sistemi normativi basati sul concetto di "consenso informato".

Nell'ottica non solo del GDPR ma anche della nuova legislazione europea, dal *Digital Services Act* e *Data Markets Act* fino al *Data Governance Act* e *Data Act*, la tendenza è quella di rendere l'utente sempre più parte dell'economia digitale e anch'esso protagonista dei trattamenti che estraggono valore dalle informazioni a lui riferite[78].

---

[72] European Parliament, *Regulating targeted and behavioural advertising in digital services. How to ensure users' informed consent*, 30 August 2021.

[73] *Ex multis*, le decisioni della Data Protection Commission irlandese: del 31 dicembre 2022, contro Meta Platforms Ireland Limited con riferimento ai servizi Facebook e Instagram; del 12 gennaio 2023, contro WhatsApp Ireland Limited; Garante per la protezione dei dati personali, provvedimento n. 248 contro TikTok del 7 luglio 2022, doc. web n. 9788429.

[74] EDPB, *Linee guida 8/2020 sul targeting*, cit.; EDPB, *Binding Decision 3/2022 on Irish SA and Meta*, cit.

[75] EDPB, *Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them*, version 2.0, 14 February 2023.

[76] V. Ricciuto, *L'equivoco della privacy. Persona vs. dato personale*, Napoli, 2022, 87 e ss, che, a proposito, afferma: «per il diritto il dato circola e può circolare *solo* e *se* "protetto": se e in quanto, cioè, trattato coerentemente e conformemente con il particolare statuto normativo che definisce presupposti, limiti, e condizioni della possibilità (*rectius*: del diritto) di compiere sullo stesso operazioni di trattamento, così come delineato dal GDPR. Sicché proteggere i dati personali non equivale (né deve equivalere) a limitare la loro circolazione/trattamento nei processi di impresa in ragione di un'aprioristica prevalenza degli interessi e dei diritti della persona rispetto al fenomeno circolatorio ed agli ulteriori interessi ad esso sottesi e da esso implicati. Protezione dei dati personali e loro circolazione si integrano; il dato personale protetto non è il dato segreto, inaccessibile, ma il dato che circola e viene trattato. Il che, detto in altri termini, equivale a dire che la libera circolazione dei dati garantita dall'ordinamento e meritevole di tutela è una circolazione protetta, perché protetto è il suo oggetto».

[77] G. d'Ippolito, *Online Behavioural advertising e protezione dei dati personali*, in D. Buzzelli-M. Palazzo (a cura di), *Intelligenza artificiale e diritti della persona*, Pisa, 2022, 125 ss.

[78] D. Poletti, *Il controllo dell'interessato e la strategia europea sui dati*, in *Osservatorio sulle fonti*, 2, 2023, 367 ss.

L'elemento da considerare, passando quindi al tema della regolazione delle piattaforme digitali, è la necessità di tener conto della scelta dell'utente, tanto antecedente all'inizio del trattamento, quindi sotto forma di consenso, quanto che sia in costanza di questo, quindi sotto forma di esercizio dei diritti, in particolare quale diritto di opposizione *ex* art. 21 del Regolamento.

Il consenso costituisce quindi un'ulteriore variabile del mercato, suscettibile di incidere sul modello di business adottato dal fornitore del servizio e non vincolabile tramite condizioni contrattuali perché esercizio di un diritto fondamentale: il corretto trattamento dei dati personali che si esplica nel più ampio potere di controllo sugli stessi[79]. Valori, questi, in linea anche con l'art. 41 della Costituzione italiana laddove subordina l'iniziativa economia all'utilità sociale e alla dignità umana[80].

Dinanzi soggetti che hanno accumulato un potere economico che nemmeno gli Stati riescono a fronteggiare, continuare a ritenere il contratto lo strumento migliore per contemperare le contrapposte esigenze, tanto più in un contesto in cui anche i tradizionali rimedi contro l'asimmetria informativa (come gli obblighi di trasparenza o le clausole vessatorie) si rivelano una tutela debole o formale, rischia di agevolare il consolidamento di un ecosistema squilibrato a vantaggio non solo della primazia dell'economia sul diritto ma a vantaggio di pochi grandi soggetti nei confronti della moltitudine di attori oggi operanti sui mercati digitali (non solo utenti e *start-up* o piccoli operatori come i produttori di app, i *content creator* o *influencer*, ma anche soggetti che si comportano da intermediari[81] o finanche soggetti pubblici o svolgenti compiti di interesse pubblico).

Ecco perché le norme contenute nel GDPR sono solo il principale esempio di un nuovo modo di legiferare che, in linea con le esigenze del costituzionalismo digitale, pone dei paletti all'iniziativa economia a presidio di principi che non solo tutelano la persona ma presidiano un più ampio sistema di valori[82]. Principi ovviamente non derogabili

[79] Come noto, il corretto trattamento dei dati personali quale diritto fondamentale è rinvenibile nell'art. 8, c. 1, della Carta dei diritti dell'Unione europea e nell'art. 16, par. 1, del TFUE. In generale si vedano: M. Bassini, *Il diritto costituzionale alla "privacy" nel prisma dell'evoluzione tecnologica*, in *Diritto costituzionale*, 1, 2023, 83 ss.; O. Pollicino, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *Federalismi.it*, 3, 2014, 1 ss.; C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 22, 2018, 1 ss.

[80] Ma anche alla salute, all'ambiente, alla sicurezza, alla libertà. In linea generale, inoltre, è anche possibile rilevare che, tradizionalmente, l'art. 1322 c.c. subordina l'autonomia negoziale ai «limiti imposti dalla legge» e agli «interessi meritevoli di tutela secondo l'ordinamento giuridico».

[81] Si veda, a proposito la segnalazione di Hoda contro Google per abuso di posizione dominante nel settore della portabilità dei dati: AGCM, provvedimento 18 luglio 2023, n. 30736, cit.

[82] Autorevole dottrina parla, a proposito, del modello del c.d. "consenso remunerato", ossia di un sistema di integrazione tra strumenti privatistici e strumenti pubblicistici che consente di far coesistere la libera circolazione dei dati con un alto livello di protezione dei diritti coinvolti, e in particolare del diritto fondamentale alla protezione dei dati personali sancito dall'art. 8, c. 1, della Carta dei diritti fondamentali UE, nonché del modello del "contratto conformato", ossia dell'accordo negoziale a cui l'ordinamento pone specifiche limitazioni e garanzie a tutela di un'adesione all'intesa contrattuale che sia espressione libera e consapevole di autonomia nelle scelte. G. Resta, *Contratto e diritti fondamentali*, in *Enc. dir.,* I, Milano, 2021, 304 ss. Altra autorevole dottrina parla di "diritto privato regolatorio" e di "contratto funzionalizzato" per indicare che il contratto stipulato dai privati è vagliato in relazione alla sua compatibilità con il sistema degli scambi nel quale esso si inserisce (il mercato) ed è altresì conformato *ab externo* rispetto alle esigenze e ai valori che caratterizzano l'assetto di *quel* mercato. V. Ricciuto, *L'equivoco della privacy,* cit., 83 ss; Infine, altra dottrina parla di "contratto amministrato" dalle Autorità amministrative indipendenti che, in presenza di una regolazione del mercato tendente a instaurare e

dall'autonomia contrattuale e che dovrebbero essere considerati dal mercato come la bussola per sviluppare modelli di business più sostenibili e rispettosi dell'autodeterminazione della persona[83].

In questo schema regolatorio, l'esigenza di una rinnovata e più forte collaborazione delle autorità di controllo, così come di un'applicazione trasversale delle normative coinvolte, è strumentale alla tutela di valori come la concorrenza, il corretto trattamento dei dati personali, il pluralismo, ecc. E deriva appunto dalla consapevolezza di dover dare all'utente, alla persona, al cittadino digitale, una tutela effettiva e completa.

La normativa europea fa dell'utente un attore non secondario dei mercati digitali e questa qualifica deve essere valorizzata, non sminuita.

Senza questa consapevolezza, senza riconoscere agli utenti un reale e immediato potere di incidere sul funzionamento dei servizi digitali, così come alle autorità di collaborare per riconoscere allo stesso una tutela effettiva, a poco servono i diritti e i rimedi *ex post* e, ancor meno, aumentare gli obblighi informativi.

garantire principi di rilievo costituzionale (concorrenza, pluralismo, ecc.) nonché dell'inadeguatezza dei privati nell'attuare loro stessi tali principi, rinviene nelle Autorità indipendenti il potere di conformare i contratti ai valori ai quali è improntato l'assetto di un dato mercato. C. Solinas, *Il contratto "amministrato". La conformazione dell'operazione economica privata agli interessi generali*, Napoli, 2018, 207 ss.

[83] Sfida effettivamente colta da alcuni operatori che fanno, meritoriamente, della protezione dei dati personali un elemento di concorrenza: dagli *add-on* per il blocco o la selezione di cookie, a browser che aumentano il potere di controllo sui propri dati o sistemi operativi che riconoscono all'utente la scelta se inibire il tracciamento pubblicitario delle app sui propri smartphone, fino ai tentativi e alle richieste di "*sandbox*" regolatorie per sviluppare sistemi di profilazione pubblicitaria più in linea con i principi europei.

Accesso al registro dei titolari effettivi e tutela dei dati personali*

Laura Tadiotto

Corte di giustizia dell'Unione europea, 22 novembre 2022, cause riunite C-37/20 e C-601/20, *Luxembourg Business Registers e Sovim*

Il diritto dei terzi di accedere ai dati personali contenuti nel registro dei titolari effettivi deve essere riconosciuto in misura proporzionata e per quanto strettamente necessario al fine di prevenire il riciclaggio di denaro e il finanziamento del terrorismo.
L'accesso al pubblico "in ogni caso" dei dati personali contenuti nel registro dei titolari effettivi previsto dalla direttiva (UE) 2015/849 (come modificata dalla direttiva (UE) 2018/843) vìola l'art. 52 della Carta dei diritti fondamentali dell'Unione europea, poiché non è proporzionato né limitato allo stretto necessario per prevenire il riciclaggio di denaro e il finanziamento del terrorismo.

Sommario

Keywords

accesso ai dati personali - data protection - Carta dei diritti fondamentali dell'Unione europea - pubblici registri - registro dei titolari effettivi.

1. Premesse

La decisione della Grande Sezione della Corte di giustizia dell'Unione europea (di seguito anche "CGUE") del 22 novembre 2022 offre indicazioni fondamentali per l'inquadramento del neo-nato registro dei titolari effettivi. La pronuncia in commento trae origine da due rinvii pregiudiziali operati ai sensi dell'art. 267 TFUE dal Tribunale circoscrizionale di Lussemburgo[1]. Tali rinvii pregiudiziali sono volti a vagliare la compatibilità della normativa sull'accesso al pubblico delle informazioni sulla titolarità

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".
[1] I rinvii pregiudiziali in questione sono stati proposti il 24 gennaio 2020 e il 13 ottobre 2020 dal *Tribunal d'arrondissement de Luxembourg* nei procedimenti C-37/20, *WM* c. *Luxembourg Business Registers*, e C-601/20, *Sovim SA* c. *Luxembourg Business Registers*.

effettiva contenuta nella IV Direttiva AML (così come da ultimo modificata ad opera della V Direttiva AML)[2] con il sistema europeo sulla protezione dei dati personali, segnatamente con i diritti fondamentali sanciti dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (d'ora in poi anche più semplicemente indicata come "Carta") sul rispetto, rispettivamente, della vita privata e familiare e la tutela dei dati personali, nonché a chiarire l'interpretazione di alcuni concetti fondamentali dell'art. 30, par. 9, della predetta direttiva, quali la nozione di "circostanze eccezionali" e "rischio proporzionato".

La Corte di giustizia dell'Unione europea si pronuncia su una delle questioni pregiudiziali proposte, considerando le altre assorbite, ed opera una ridefinizione dell'accesso al pubblico delle informazioni contenute nel registro dei titolari effettivi.

A seguito della decisione della Corte, diversi Stati membri hanno già adattato il proprio meccanismo di accesso alle informazioni sulla titolarità effettiva. Tuttavia, gli esiti espressi dalla Corte, sebbene rivoluzionari, non esauriscono – come vedremo – l'insieme dei punti di contatto tra la disciplina AML sull'accesso alle informazioni sulla titolarità effettiva e la normativa in materia di protezione dei dati personali, ed in particolare il regolamento generale sulla protezione dei dati (d'ora in poi anche "GDPR[3]").

Da ultimo, la pronuncia in commento offre uno spunto di riflessione sull'inquadramento del registro dei titolari effettivi in rapporto agli altri sistemi pubblicitari (d'impresa). Tale circostanza assume particolare rilievo in un sistema come quello italiano, in cui il registro sulla titolarità effettiva è configurato quale sezione del registro delle imprese tenuto dalla Camera di Commercio (di seguito anche "CCIAA").

2. Il registro dei titolari effettivi. Cenni introduttivi

Come noto, l'istituzione di pubblici registri contenenti informazioni sulla titolarità effettiva è stata prevista dalla IV Direttiva AML/CFT[4], al fine di promuovere la trasparenza e quindi contrastare l'utilizzo abusivo di soggetti giuridici per il riciclaggio o il finanziamento del terrorismo[5]. Una volta resi operativi i registri nazionali, la stessa direttiva prevede la messa in opera di un sistema di interconnessione degli stessi[6], allo scopo di accrescere la capacità informativa a livello eurounitario. La predetta intercon-

[2] In particolare, l'art. 1, punto 15, lett. *c)*, della direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio (c.d. V Direttiva AML o AMLD V) a modifica dell'art. 30, par. 9, della direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo (c.d. IV Direttiva AML o AMLD IV).

[3] Acronimo di *General Data Protection Regulation*, ossia il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[4] Acronimo per *Anti Money Laudering* e *Combating the Financing of Terrorism*.

[5] Sull'individuazione del titolare effettivo si veda G. Arcella - S. Carioni - M. Nastri - L. Piffaretti, *Studio 1_2023 B – La ricerca del titolare effettivo*, in *notariato.it*, 22 febbraio 2023.

[6] Regolamento di esecuzione (UE) 2021/369 della Commissione europea, relativo alle specifiche tecniche e alle procedure necessarie per il sistema di interconnessione dei registri centrali di cui alla direttiva (UE) 2015/849.

nessione è basata su un sistema decentralizzato, in forza del quale è possibile addivenire alle informazioni sulla titolarità effettiva così come registrate a livello nazionale.
Venendo alla questione dell'accesso, si ricorderà forse che secondo la versione originaria della IV Direttiva AML questo doveva ritenersi assicurato, oltre che alle autorità competenti e ai soggetti obbligati all'adeguata verifica della clientela, a qualunque soggetto in grado di dimostrare un "interesse legittimo"[7]. L'accesso al pubblico risultava pertanto vincolato dalla prova del citato concetto, non sempre di facile ed omogenea applicazione pratica.
La disciplina in parola, contenuta all'art. 30 della AMLD IV, è stata riformata dalla V direttiva antiriciclaggio[8], che nell'incrementare la lista dei soggetti che possono accedere «in ogni caso» alle risultanze del registro ha aggiunto il "pubblico" (c. 5, lett. *c*), salvo poi precisare che l'accesso al pubblico deve riguardare almeno talune informazioni evidentemente considerate essenziali, salva la facoltà per gli Stati membri «alle condizioni previste dal diritto nazionale» di ampliare l'accesso anche a «informazioni aggiuntive che consentono l'identificazione del titolare effettivo». Soltanto eccezionalmente, infine, è data ai singoli Stati membri la possibilità, a seguito di una valutazione casistica, di limitare l'accesso dei dati da parte del pubblico, laddove sussista un «rischio sproporzionato di frode, rapimento, ricatto, estorsione, molestia, violenza o intimidazione» oppure qualora «il titolare effettivo sia un minore di età o altrimenti incapace per legge». L'estensione dell'accesso al pubblico è motivata dal possibile apporto della società civile nella prevenzione al riciclaggio di denaro e al finanziamento del terrorismo, rafforzando ulteriormente un sistema di trasparenza in materia.
Proprio l'accesso alle informazioni sulla titolarità effettiva delineatosi a seguito della V direttiva ha determinato la pronuncia della CGUE in commento, pronuncia che di fatto interessa anche i lavori della VI direttiva antiriciclaggio[9], ora allo studio, che sembrerebbe voler riproporre lo stesso regime sanzionato dalla Corte[10].

3. La decisione della Grande Sezione della Corte di giustizia

La Corte stabilisce l'invalidità delle modifiche apportate nel 2018 alla IV direttiva in punto di accesso al pubblico alle informazioni sulla titolarità effettiva, in ragione del mancato rispetto agli artt. 7, 8 e 52 della Carta.
Il ragionamento della Corte muove dalla constatazione per cui le informazioni sulla titolarità effettiva comprendono dati su persone fisiche identificate, ovvero i titolari effettivi. Di conseguenza, l'accesso al pubblico alle suddette informazioni incide sul

[7] Art. 30, par. 5, direttiva (UE) 2015/849.

[8] Art.1, punto 15, direttiva (UE) 2018/843.

[9] COM (2021) 423 final, Proposta di direttiva relativa ai meccanismi che gli Stati membri devono istituire per prevenire l'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo e che abroga la direttiva (UE) 2015/849, 2021/0250 (COD), 21 luglio 2021, consultabile in *eur-lex.europa.eu* .

[10] Artt. 12 e 13 della Proposta sopra citata, rubricati, rispettivamente, «norme specifiche di accesso ai registri dei titolari effettivi per il pubblico» e «eccezioni alle norme di accesso ai registri dei titolari effettivi».

rispetto alla vita privata e familiare di cui all'art. 7 della Carta; esso determina inoltre un trattamento di dati personali ai sensi dell'art. 8. Potendo quindi i terzi, in quanto "pubblico", accedere ai dati contenuti nei registri dei titolari effettivi, si concreta un'ingerenza nei diritti fondamentali di questi ultimi quali tutelati dagli artt. 7 e 8.

Successivamente la Corte vaglia la gravità della suddetta ingerenza. Sin da tale valutazione, emergono diversi profili di criticità del sistema di accesso, in seguito puntualizzati dalla Corte. Anzitutto, il novero dei dati personali accessibili è rimesso alle legislazioni nazionali. Essi sono inoltre accessibili ad un numero di soggetti indefinito ed illimitato di soggetti. Infine, l'accesso pubblico non è sorretto da alcun effettivo presidio rispetto ad un utilizzo abusivo delle informazioni contenute nei registri in questione. Ciò conduce la Corte a qualificare come "grave" l'ingerenza nei diritti *ex* artt. 7 e 8 costituita dall'accesso al pubblico, così come definito dalle direttive AML del 2015 e del 2018.

A questo punto, però, entra in gioco l'eccezione di cui all'art. 52 della Carta, secondo cui le limitazioni dei diritti fondamentali possono considerarsi legittime laddove i) risultino «necessarie» e rispondano «effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere diritti e le libertà altrui»; ii) siano previste dalla legge, e iii) rispettino il principio di proporzionalità ed il contenuto essenziale dei diritti. La CGUE analizza dunque i singoli presupposti per ritenere legittima un'ingerenza ai diritti fondamentali previsti dalla Carta.

Incontestabile è il rispetto del principio di legalità, trattandosi di una limitazione che trova la sua fonte in un atto dell'Unione (la IV Direttiva AML, per l'appunto).

Quanto al contenuto essenziale dei diritti fondamentali *ex* artt. 7 e 8, la Corte rileva che l'accessibilità riguarda le informazioni aventi una «relazione adeguata con le finalità della direttiva», per cui non discenderebbe alcun pregiudizio al contenuto essenziale dei citati diritti.

Nell'individuare l'obiettivo di interesse generale riconosciuto dall'Unione europea, la CGUE richiama i considerando della direttiva del 2018[11], laddove si evidenzia come il pubblico accesso consente alla società civile di contribuire «a mantenere la fiducia nell'integrità delle operazioni commerciali e del sistema finanziario», nonché «a combattere l'uso improprio di società, altri soggetti giuridici e istituti giuridici per riciclare denaro e finanziare il terrorismo», oltre che di agevolare le indagini sui reati in questione. L'accesso pubblico alle informazioni sulla titolarità effettiva rafforza pertanto la trasparenza, al fine ultimo di prevenire il riciclaggio e il finanziamento del terrorismo. In ciò consisterebbe il requisito dell'obiettivo di interesse generale, necessario per giustificare la limitazione ai diritti di cui agli artt. 7 e 8 della Carta.

Il cuore della decisione della Corte verte però sulla valutazione dei presupposti di necessità e di proporzionalità del pubblico accesso[12], così come disciplinato dalle direttive in materia. Rispetto al primo, l'accesso del pubblico alle informazioni sulla titolarità effettiva non è reputato dalla Corte strettamente necessario allo scopo di prevenire

[11] In particolare, i considerando 30 e 31.

[12] Sui requisiti di proporzionalità e stretta necessità di cui all'art. 52 della Carta si veda L. Dalla Corte, *On proportionality in the data protection jurisprudence of the CJEU*, in *International Data Privacy Law*, 12, 2022, 262 ss.

il riciclaggio e il finanziamento del terrorismo. Ciò anche alla luce del rilievo per cui sono primariamente preposti al contrasto dei suddetti reati le pubbliche autorità ed i soggetti tenuti ad obblighi specifici in materia, ma non la società civile. Ne deriva che l'ingerenza nei confronti dei diritti fondamentali di cui agli artt. 7 e 8 della Carta non può dirsi limitata allo stretto necessario per il perseguimento dell'obiettivo di interesse generale specificato.

Il rispetto del requisito di proporzionalità è valutato mediante un bilanciamento tra lo specifico obiettivo di interesse generale perseguito ed i diritti fondamentali in questione, considerando l'esistenza di eventuali garanzie rispetto a rischi di abusi. A questo proposito, la Corte osserva come – contrariamente a quanto affermato nei considerando nel 2018[13] – la direttiva preveda solo un elenco esemplificativo di dati personali accessibili al pubblico, facoltizzando gli Stati membri a rendere accessibili anche informazioni aggiuntive. Dall'altro lato, la CGUE non ravvisa sufficienti garanzie contro il rischio di un utilizzo abusivo delle informazioni accessibili al pubblico nelle previsioni di cui ai paragrafi 5-*bis* e 9 dell'art. 30 della direttiva. Tali disposizioni riguardano, rispettivamente, la facoltà per gli Stati membri di condizionare l'accesso alle informazioni sulla titolarità effettiva ad una preventiva registrazione *online* e di derogare al pubblico accesso in presenza di circostanze eccezionali ove il singolo soggetto sia esposto ad un rischio sproporzionato di frode, rapimento, ricatto, estorsione, molestia, violenza o intimidazione. Le misure appena delineate non costituiscono una garanzia sufficiente per proteggere efficacemente i dati personali accessibili al pubblico contro il rischio di un loro utilizzo abusivo, proprio perché rimesse alla mera facoltà del singolo Stato membro. Di conseguenza, la Corte non ritiene sussista un bilanciamento tra l'obiettivo di interesse generale ed i diritti fondamentali considerati.

L'*iter* seguito dalla CGUE – come sopra sinteticamente ricostruito – si fonda sull'applicazione dell'art. 52 della Carta al caso specifico, a cui consegue una pronuncia di invalidità in ragione sia dell'assenza di un rapporto di stretta necessità del sistema del pubblico accesso con il fine di prevenire il riciclaggio di denaro e il finanziamento del terrorismo, e sia anche di un'asserita sproporzione dell'ingerenza consumata nei confronti dei diritti di cui agli artt. 7 e 8 della Carta. Non è invece espressamente e compiutamente valutata la compatibilità del sistema di accesso ai dati personali contenuti nel registro dei titolari effettivi con la disciplina contenuta nel GDPR.

Inoltre, all'esito della pronuncia, è possibile rinvenire un accenno ai rapporti tra i dati contenuti nel registro dei titolari effettivi e le informazioni pubblicate nei registri inerenti alla pubblicità commerciale. In particolare, la Corte ritiene inconferente il riferimento, operato dalla Commissione, alla sentenza *Manni* del 9 marzo 2017[14], in materia di pubblicità obbligatoria delle società e dei relativi rappresentanti legali prevista dalla direttiva 68/151/CEE rispetto alle questioni sottopostole. La CGUE rende quindi esplicita la differenza tra la pubblicità d'impresa e l'accesso pubblico alle informazioni

[13] Considerando 34 della direttiva (UE) 2018/843, secondo cui «L'insieme di dati da mettere a disposizione del pubblico dovrebbe essere limitato, definito in maniera chiara e tassativa».

[14] CGUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Manni* (2017); in senso analogo si vedano le conclusioni dell'Avvocato generale, Yves Bot, dell'8 settembre 2016 relative alla causa C-398/2015, in *curia.europa.eu* .

sulla titolarità effettiva in ragione delle diverse finalità perseguite dai *corpus* normativi di riferimento e la diversa portata dei dati personali interessati.
In particolare, i dati personali contenuti nel registro delle imprese ed accessibili ai terzi per finalità pubblicitarie riguardano le persone fisiche in quanto membri degli organi della persona giuridica e sono strettamente limitati al nome, cognome, codice fiscale e funzione ricoperta. Inoltre, il predetto accesso ai terzi è volto a preservare la funzione essenziale del registro, fornendo un quadro statico e storico dell'organizzazione del soggetto giuridico iscritto al fine di mettere a disposizione delle terze informazioni giuridicamente cruciali per rapportarsi con i soggetti iscritti. Di conseguenza, nella pubblicità d'impresa sembrano essere rispettati i principi di stretta necessità e proporzionalità di accesso ai dati personali, diversamente da quanto specificato dalla CGUE in punto di accesso alle informazioni sulla titolarità effettiva.
Tale differenziazione assume particolare valore in un sistema come quello italiano in cui il registro dei titolari effettivi non è formalmente configurato quale registro autonomo, bensì costituisce "parte" del Registro delle imprese tenuto dalle Camere di Commercio. In Italia, il registro dei titolari effettivi consiste infatti in due sezioni del registro delle imprese: una sezione autonoma relativa alle imprese dotate di personalità giuridica e alle persone giuridiche private; una sezione speciale per i trust e gli istituti giuridici affini. Diversamente, in altri Stati membri, le informazioni sulla titolarità effettiva sono contenute in un registro *ad hoc*, distinto rispetto al sistema di pubblicità d'impresa; ciò avviene, ad esempio, in Germania, in cui il registro, tenuto a livello federale, viene peraltro denominato *Transparenzregister*, ossia "registro per la trasparenza".
La peculiare valutazione effettuata dalla CGUE sull'accesso alle informazioni sulla titolarità effettiva rispetto a quanto avviene nelle ipotesi di pubblicità legale afferente ai dati personali nell'ambito di società ed altre entità giuridiche valorizza nuovamente il carattere anomalo[15] delle sezioni del registro delle imprese adibite a conservare le informazioni sui titolari effettivi rispetto alle altre sezioni del registro delle imprese. Si pone quindi la necessità di considerare tale anomalia nell'applicazione alle sezioni sulla titolarità effettiva dei principi e delle disposizioni che regolano il funzionamento del registro delle imprese.

4. L'accesso al registro dei titolari effettivi secondo il GDPR

Il rapporto tra il sistema di accesso al registro dei titolari effettivi e il GDPR è trattato incidentalmente e parzialmente dalla decisione in commento[16], venendosi solo a precisare che la raccolta, la conservazione e la messa a disposizione di informazioni secondo la Direttiva AML/CFT deve avvenire in modo "pienamente conforme" al GDPR. Nulla si dice invece su come questo coordinamento debba avvenire. La scelta della locuzione sopra citata – "pienamente conforme" – potrebbe indurre a sostene-

[15] C. Ibba, *Il registro delle imprese*, Milano, 2021, 35.

[16] La Corte non ritiene necessario pronunciarsi sulla terza questione proposta nella causa C-601/20, visto l'esito invalidante della prima questione affrontata.

re la recessività della disciplina sull'accesso ai dati della titolarità effettiva rispetto a quanto previsto dal GDPR. Sì che quando gli Stati dovessero decidere di riformare il sistema di accesso al registro dei titolari effettivi, questi non potranno non considerare la disciplina delineata dal GDPR in materia di protezione dei dati personali.

Sulla base di tali preliminari osservazioni, alcuni aspetti cardinali del GDPR – ossia il rispetto dei principi applicabili al trattamento dei dati personali di cui all'art. 5 del GDPR, la protezione dei dati in caso di impostazione predefinita ed il trasferimento dei dati verso Paesi terzi o organizzazioni internazionali - sono di seguito rapportati al sistema di accesso ai dati sulla titolarità effettiva.

Anzitutto, il trattamento dei dati personali relativi alla titolarità effettiva deve rispettare il principio di liceità del trattamento[17], per cui deve essere individuata la base giuridica del trattamento stesso. Nell'ambito della IV Direttiva AML, il trattamento dei dati personali è considerato di interesse pubblico, come previsto dalla normativa unionale e come implementato a livello nazionale[18].

Quanto al principio di limitazione della finalità del trattamento[19], è chiaro che l'accesso pubblico non consente al titolare del trattamento[20] di garantire che l'accesso sia limitato allo scopo di contrastare il riciclaggio di denaro e il finanziamento del terrorismo. Sul punto, dal provvedimento della CGUE non sembra emergere alcuna indicazione, ma è chiaro che la predisposizione di un meccanismo di accesso condizionato o basato su un interesse legittimo può avvicinare la misura allo scopo.

Il principio di minimizzazione dei dati[21] riveste rilevanza centrale alla luce dell'iter argomentativo seguito dalla Corte, poiché racchiude i presupposti di stretta necessità e proporzionalità di cui all'art. 52 della Carta, fulcro della decisione. Quanto statuito dalla CGUE rappresenta pertanto una guida anche per l'interpretazione all'applicazione del principio di minimizzazione dei dati di cui al GDPR nello specifico settore dell'accesso ai dati per finalità antiriciclaggio.

La disposizione del GDPR relativa alla protezione dei dati *by design*[22] specifica che il titolare del trattamento deve adottare misure tecniche ed organizzative adeguate per rendere accessibili i dati personali ad un numero indefinito di persone soltanto mediante un intervento del soggetto i cui dati sono trattati. Rispetto a tale disposizione, l'accesso al pubblico risultante dalla decisione della CGUE necessita di essere reso conforme alla suddetta disposizione. Poiché le suddette misure devono essere predisposte dal titolare del trattamento, conformemente al principio di responsabilizzazione di quest'ultimo, esse dovranno essere disciplinate a livello nazionale. Infine, se la di-

[17] Art. 5, par. 1, lett. *a)*, e art. 6 GDPR.

[18] L'Italia esplicita la base giuridica del trattamento delle informazioni sulla titolarità effettiva all'art. 2, c. 6-*bis*, del d. lgs. 231/2007.

[19] Tale principio è previsto all'art. 5, par. 1, lett. *b)*, GDPR; quest'ultima disposizione prevede, tra l'altro, che i dati personali devono essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità».

[20] Nell'ordinamento italiano, il titolare del trattamento, come definito all'art. 4, par. 1, n. 7), GDPR, sarebbe la Camera di Commercio territorialmente competente a ricevere i dati sulla titolarità effettiva.

[21] Art. 5, par. 1, lett. *c)*, GDPR, secondo cui i dati personali devono essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono stati trattati».

[22] Art. 25 GDPR ed in particolare l'ultima parte del secondo paragrafo.

sciplina AML, in ragione delle finalità dalla stessa perseguite, non sembra preoccuparsi dell'ubicazione geografica del pubblico, in materia di protezione dei dati personali è specificata una disciplina per il trasferimento di dati personali verso Paesi terzi od organizzazioni internazionali[23]. La regolamentazione sul punto deve quindi essere applicata anche nell'ambito dell'accesso ai registri sulla titolarità effettiva, come emerge dall'art. 44 GDPR. Tuttavia, ai sensi dell'art. 49 GDPR, il trasferimento dei dati sulla titolarità effettiva non richiede né la valutazione di adeguatezza della Commissione *ex* art. 45 GDPR, né le adeguate garanzie di cui all'art. 46 GDPR poiché il suddetto trasferimento è «necessario per importanti motivi di interesse pubblico»[24]. Sul punto, la decisione della Corte ha un importante valore interpretativo, dal momento che in essa viene definito il parametro di necessarietà per l'interesse pubblico perseguito. Difatti, soltanto l'accesso alle informazioni sulla titolarità effettiva come interpretato dalla CGUE è tale da giustificare le deroghe di cui all'art. 49 GDPR. Diversamente, l'accesso "in ogni caso" previsto dalla direttiva del 2018 avrebbe richiesto la decisione di adeguatezza *ex* art. 45 GDPR e le garanzie *ex* art. 46 GDPR.

5. Iniziative a livello nazionale

La decisione in commento ha comportato – come era ovvio che fosse – la sospensione del regime di accesso libero ai registri dei titolari effettivi già operativi nel territorio unionale e l'avvio di un processo di revisione finalizzato all'adeguamento del sistema ai principi fissati dalla Corte. Ne sono conseguiti una pluralità di approcci, fra cui spiccano l'esempio tedesco ed irlandese, di cui si dirà allo scopo di identificare gli indirizzi pratici più confacenti, oltre che alla normativa sulla protezione dei dati personali, anche alle esigenze pratiche degli operatori che utilizzeranno il registro in questione. Ciò in ragione anche della particolare situazione in cui versa l'Italia, ove su pressione delle istituzioni europee e dopo l'avvio di una procedura di infrazione[25], il legislatore si è trovato costretto ad adottare un sistema dallo stesso espressamente definito "provvisorio". Diverso il caso della Germania[26], dove dopo la sentenza della Corte, il sistema prevede ora un regime d'accesso ai dati sulla titolarità effettiva diversificato sotto molteplici aspetti. Dal punto di vista soggettivo, sono individuati tre gruppi di soggetti autorizzati all'accesso, ossia le autorità, i soggetti obbligati e il pubblico. Quanto alle condizioni richieste, le autorità[27] possono accedere illimitatamente nell'adempimento dei loro do-

[23] Artt. da 40 a 50 GDPR.

[24] Così art. 49, par. 1, lett. *d)*, GDPR.

[25] L'infrazione in questione è INFR (2022) 2150 per il mancato recepimento della IV direttiva antiriciclaggio (così come modificata dalla V direttiva antiriciclaggio), tra cui la mancata istituzione del registro dei titolari effettivi.

[26] La disciplina nazionale sul registro sulla titolarità effettiva, denominato *Transparenzregister*, è contenuta nella legge *Gesetz zur europäischen Vernetzung der Transparenzregister und zur Umsetzung der Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Nutzung von Finanzinformationen für die Bekämpfung von Geldwäsche, Terrorismusfinanzierung und sonstigen schweren Straftaten (Transparenzregister- und Finanzinformationsgesetz)*.

[27] Ossia le autorità, i tribunali e gli organismi di cui al par. 2, c. 4, del GwG *(Behörden, Gerichte und die in*

veri; i soggetti obbligati possono accedere, nell'adempimento dei loro doveri, soltanto caso per caso[28]; infine, il pubblico deve dimostrare un interesse legittimo all'accesso. A sua volta tale interesse legittimo viene specificamente declinato: per le organizzazioni governative e i giornalisti[29], esso sussiste durante le ricerche condotte sul riciclaggio di denaro e il finanziamento del terrorismo; diversamente, il restante pubblico ha un interesse legittimo a controllare soltanto le proprie informazioni contenute nel registro. In quest'ultima ipotesi, peraltro, l'accesso alle proprie informazioni altro non è che l'esercizio del diritto di accesso in senso tecnico previsto dall'art. 15 del GDPR. Pertanto, a prescindere da una specifica disposizione sul registro in questione, ogni titolare effettivo dovrebbe poter avere accesso ai propri dati personali ivi contenuti sulla base del diritto di accesso previsto dal regolamento sulla protezione dei dati.

La declinazione offerta dallo Stato tedesco del concetto di "interesse legittimo" comporta un restringimento della nozione di "pubblico", poiché in realtà soltanto determinati soggetti possono accedere alle informazioni sulla titolarità effettiva. Un sistema di accesso così congegnato, nell'auspicio di essere conforme alla decisione della Corte, per un verso riporta al regime previsto originariamente dalla direttiva del 2015; per altro verso, supera le criticità della stessa, specificando il concetto di interesse legittimo. Ancora più granulare si presenta la nuova disciplina irlandese, costruita sulla scorta di un duplice criterio (soggettivo ed oggettivo), tanto da differenziare i dati accessibili ai diversi gruppi di soggetti.

Sotto il profilo soggettivo, in un primo gruppo di soggetti sono comprese le autorità di vigilanza e le istituzioni pubbliche, nel secondo gruppo sono inclusi i soggetti obbligati[30] ed il terzo gruppo è costituito dal pubblico. La peculiarità del sistema irlandese, ossia un accesso differenziato sotto il profilo delle informazioni consultabili, è così configurata: il primo gruppo può accedere a tutte le informazioni disponibili[31]; il novero dei dati accessibili è limitato per i soggetti obbligati[32] rispetto alla totalità dei dati archiviati nel registro ed esso è ulteriormente circoscritto per il pubblico[33]. Il regime irlandese risulta quindi introdurre una valutazione *ex ante* e standardizzata di stretta necessità e proporzionalità rispetto all'accesso ai diversi dati personali trattati nell'ambito dei registri sulla titolarità effettiva, conformemente anche al principio di minimizzazione dei dati di cui al GDPR. A differenza del sistema tedesco, quello irlandese ovvia

§ 2 Abs. 4 GwG genannten Stellen).

[28] *Verpflichteten ist der Zugang dagegen nur fallbezogen und im Rahmen ihrer Sorgfaltspflichten gestattet.*

[29] *Journalisten und Nichtregierungsorganisationen* (NGOs).

[30] Specificati quali «*designated persons required by Part 4 of the 2010 Criminal Justice (Money Laundering and Terrorist Financing) Act to conduct customer due diligence tests*».

[31] Ossia «*forename and surname; sate of birth; nationality; residential address; a statement of the nature and extent of the interest held by each beneficial owner, or the nature and extent of control exercised by, each such beneficial owner; the date on which each natural person was entered in the relevant entity's own register as a beneficial owner and the date on which each person ceased to be a beneficial owner of the entity; details of the presenter making the entry in the RBO on behalf of the company i.e. forename and surname, address, phone number, e-mail address and capacity in which they are filing*».

[32] Ossia «*forename and surname; month and year of birth; nationality; country of residence; a statement of the nature and extent of the beneficial interest held, or control exercised*».

[33] «*In accordance with the recent ruling of the Court of Justice of the European Union only the entity profile is available, but will show the number of beneficial owners filed*», in *rbo.gov.ie*.

alle criticità derivanti dal vaglio caso per caso sulla sussistenza dell'interesse legittimo all'accesso.

Entrambi i sistemi, quello tedesco e quello irlandese, seppur mediante scelte differenti, implementano la decisione della Corte cercando di adottare una soluzione attenta anche alle esigenze operative, facilitandone l'applicazione concreta.

Da ultimo, anche l'Italia ha cercato di uniformarsi all'orientamento della CGUE, sebbene il registro dei titolari effettivi non fosse ancora operativo quando la decisione è intervenuta. Il primo decreto attuativo del registro italiano dei titolari effettivi[34] - già approvato nel marzo 2022 ma di fatto mai entrato in vigore – prevedeva infatti, sulla scia del dettato della AMLD V, un sistema di accesso pubblico «previa richiesta e senza limitazioni»[35]. Tale regime è stato quindi sostituito con il decreto del Ministero delle Imprese e del Made in Italy del 12 aprile 2023[36], in forza del quale l'accesso pubblico ai dati contenuti nel registro sulla titolarità effettiva è riservato ora ai soli titolari di un «interesse giuridico rilevante e differenziato, analogamente a quanto previsto per l'accesso ai dati e alle informazioni sulla titolarità effettiva dei trust e degli istituti giuridici affini dall'art. 21, comma 4, lettera *d-bis*), del decreto legislativo 21 novembre 2007, n. 231, e quanto previsto per le imprese e le persone giuridiche private ai sensi dell'art. 21, comma 2, lettera *f*), del medesimo decreto legislativo n. 231 del 2007, nel testo vigente prima della modifica di cui all'art. 2, comma 1, lettera *g*), del decreto legislativo 4 ottobre 2019, n. 125». Va da sé che il nuovo regime, per quanto circoscritto dai rinvii normativi, implica un gravoso vaglio in caso di accesso al pubblico, gravante sugli uffici territoriali delle Camere di Commercio. Ne consegue una minore immediatezza applicativa rispetto alle soluzioni adottate in Germania e Irlanda.

Lo stesso decreto ministeriale del 2023 precisa, tuttavia, la provvisorietà della disciplina introdotta, in attesa di un provvedimento legislativo volto a dare compiuta attuazione alla pronuncia della Corte e, auspicabilmente, a tutta la regolamentazione in materia di protezione dei dati personali.

Per concludere, sebbene in Italia ed in Germania si sia tentato di precisare meglio l'interesse giustificante l'accesso al pubblico, le specificazioni introdotte sembrano in finale determinare un'ulteriore incertezza sia per gli utenti sia per i soggetti tenuti a controllare la sussistenza del suddetto interesse. Al contrario, il sistema irlandese attua le indicazioni della CGUE senza rimettere la decisione sull'accesso ad una valutazione casistica e successiva; in tal modo si è cercato di concretare una valutazione di propor-

[34] Decreto del MEF di concerto con il MISE dell'11 marzo 2022, n. 55, recante disposizioni in materia di comunicazione, accesso e consultazione dei dati e delle informazioni relativi alla titolarità effettiva di imprese dotate di personalità giuridica, di persone giuridiche private, di trust produttivi di effetti giuridici rilevanti ai fini fiscali e di istituti giuridici affini ai trust.

[35] Così art. 7, c. 1, d.m. 11 marzo 2022, n. 55.

[36] Decreto del MIMIT del 12 aprile 2023, n. 93, recante specifiche tecniche del formato elettronico della comunicazione unica d'impresa, in cui è precisato che dalla sentenza della CGUE in commento consegue la disapplicazione dell'art. 7, c. 1, d.m. 11 marzo 2022, n. 55, conformemente ai principi di cui all'art. 11 Cost.

Quanto alle ripercussioni della sentenza della CGUE sui profili tecnico-operativi, il d.m. del MIMIT del 16 marzo 2023 ha provveduto a modificare i modelli per il rilascio di certificati e copie anche digitali relativi alle informazioni sulla titolarità effettiva, mentre il d.m. del MIMIT del 20 aprile 2023 ha precisato gli importi dei diritti di segreteria.

zionalità e stretta necessità tale da non paralizzare il sistema di accesso al registro dei titolari effettivi.
Infine, i diversi approcci degli Stati membri volti a rimodulare l'accesso alle informazioni sulla titolarità effettiva, seppure tesi a conformarsi alle conclusioni raggiunte dalla CGUE, conducono a sistemi di accesso non omogenei. Tale circostanza andrà ad inficiare l'effettiva interconnessione dei registri dei titolari effettivi nel territorio unionale. Invero, l'utente dovrà confrontarsi con differenti valutazioni per accedere ai diversi registri nazionali sulla titolarità effettiva; ciò condurrà ad eventuali dinieghi ed accettazioni relativi all'identico caso concreto.

6. Conclusioni

La decisione della CGUE in commento ha reso centrale l'attenzione alla protezione dei dati personali nell'ambito della normativa antiriciclaggio, in cui in precedenza godeva di una considerazione marginale, affermando la recessività dell'esigenza di trasparenza e del controllo generalizzato da parte della società civile sulle informazioni sulla titolarità effettiva.
Il punto centrale del provvedimento è rappresentato dalla valutazione dei criteri di proporzionalità e stretta necessità richiesti dall'art. 52 della Carta per limitare i diritti fondamentali della vita privata e familiare e della tutela dei dati personali. Rispetto a tali profili, il vaglio operato dalla Corte rappresenta un *unicum* nell'ambito disciplinare di riferimento poiché per la prima volta la CGUE fornisce un indirizzo applicativo dell'art. 52 della Carta e dei principi di stretta necessità e proporzionalità nel caso specifico di trattamento dei dati personali nell'ambito della disciplina antiriciclaggio. Il provvedimento in commento rappresenta dunque un punto di partenza anche per interpretare la normativa AML conformemente al GDPR.
La sentenza della Corte ha infine ricadute specifiche sul sistema italiano dei pubblici registri ed, in particolare, sul rapporto tra il registro delle imprese e il registro dei titolari effettivi. Nonostante la collocazione di quest'ultimo nel sistema pubblicitario delle imprese, la CGUE conferma la necessità di un'autonoma valutazione in punto di accesso ai dati personali sulla titolarità effettiva, onerando e preavvisando le CCIAA territorialmente competenti di porre particolare attenzione nell'eventuale trasposizione della disciplina sul registro delle imprese alle sezioni sulla titolarità effettiva.

Il bilanciamento tra proselitismo religioso e il diritto alla protezione dei dati: un'occasione mancata per i giudici di Strasburgo?*

Alessandro Cupri

Corte europea dei diritti dell'uomo, 25 settembre 2023, ric. 31172/19, *Testimoni di Geova c. Finlandia*

Il consenso dell'interessato è un requisito necessario e appropriato alla raccolta e al trattamento dei dati nel contesto di attività di predicazione e di proselitismo religioso svolti dai Testimoni di Geova al fine di prevenire la divulgazione o comunicazione di dati personali e sensibili.

Sommario

Keywords

tutela dei dati – libertà religiosa – proselitismo – consenso – Testimoni di Geova

1. Cenni introduttivi

Di recente, la Corte europea dei diritti dell'uomo si è pronunciata sulla disciplina da applicare alla raccolta e al trattamento dei dati personali ottenuti da una congregazione religiosa durante le attività di predicazione svolte dai suoi membri porta a porta[1]. Per affrontare una questione così peculiare, i Giudici di Strasburgo hanno dovuto individuare il delicato punto di equilibrio che, all'interno di ogni società democratica e pluralista, giustappone l'esercizio della libertà di religione al rispetto della vita privata – ossia di diritti, come noto, garantiti dalla Convenzione del 1950 (o CEDU)[2].

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

1 CEDU, *Testimoni di Geova c. Finlandia*, ric. 31172/19 (2023).

2 Ivi, §§ 63 e 80. Si veda sul punto in dottrina J. Martínez Torrón, *Religious Liberty in European Jurisprudence*, in M. Hill (a cura di), *Religious Liberty and Human Rights*, Cardiff, 2002, 100. Inoltre, più ampiamente sul tema si veda G. Gomez, *La* privacy *della mente: alcune riflessioni sul rapporto tra protezione dei dati personali e*

2. L'antefatto

Il caso trae origine da una istanza presentata nel 2000 da alcuni cittadini finlandesi all'*Ombudsman* nazionale[3]. Per svolgere in modo sistematico ed efficace la loro attività di proselitismo, diversi membri della congregazione dei Testimoni di Geova trascrivevano e conservavano le più diverse risposte ricevute dalle persone conosciute nel corso della predicazione porta a porta. Secondo i cittadini interessati, gli appunti così raccolti rappresentavano però – sebbene in modo rudimentale e limitato negli scopi – una vera e propria forma di raccolta e conservazione di dati personali. In quanto tale, essi avrebbero quindi dovuto rispettare la disciplina vigente in materia, volta a prevenire qualsiasi divulgazione indesiderata almeno dei dati sensibili. In particolare, l'istanza evidenziava come i Testimoni di Geova avrebbero dovuto acquisire il consenso alla raccolta e al trattamento dei dati direttamente dalle persone contattate durante le loro attività[4]. L'*Ombudsman* sposava la tesi così suggerita, stabilendo che, anche nell'ipotesi di dati ottenuti in seguito ad attività di proselitismo, la loro raccolta e conservazione può avvenire solo con il consenso esplicito degli interessati. In quest'ottica, inoltre, la necessità di ottenere il consenso non può venir meno né in ragione del fatto che le congregazioni locali dei Testimoni utilizzavano un sistema di archiviazione manuale dei nomi e degli indirizzi delle persone contattate; né in quanto la raccolta di queste informazioni aveva il solo scopo di rispettare la volontà di coloro che non desideravano essere nuovamente contattati. Di conseguenza, conclude l'*Ombudsman*, l'attività di proselitismo svolta nelle modalità descritte si traduce in una vera e propria raccolta e conservazione di dati personali.

Non è difficile intuire le conseguenze di questo approccio: nel 2013 l'*Ombudsman* chiede al «Comitato dei dati personali» finlandese di vietare ai Testimoni di Geova – pena una sanzione pecuniaria – la raccolta e la conservazione dei dati fatta senza il consenso esplicito dell'interessato[5]. Un simile provvedimento si rende necessario poiché, in assenza del consenso esplicito, l'attività in questione vìola il diritto al rispetto della vita privata di cui all'art. 8 CEDU. Il Comitato accoglie la richiesta; la comunità dei Testimoni di Geova, di conseguenza, impugna la decisione dinanzi al Tribunale amministrativo di Helsinki: per la ricorrente, la raccolta dei dati aveva infatti il solo scopo di distinguere chi era interessato a conoscere meglio il credo dei Testimoni da coloro i quali, al contrario, non lo erano[6].

Dinanzi a questa posizione, il Tribunale amministrativo adotta un approccio nettamente diverso da quello dell'*Ombudsman* e del Comitato: il Giudice amministrativo sposta infatti l'attenzione dalle tutele poste a garanzie dei dati personali a una questione di altro tenore. Per il Tribunale amministrativo l'attività di predicazione costituisce

libertà di pensiero, in *Stato, Chiese e pluralismo confessionale*, 17, 2020, 115 ss.

[3] Per una ricostruzione dettagliata sulle varie pronunce che hanno condotto alla Corte europea dei diritti dell'uomo si veda § 5 ss.

[4] Cfr., sul punto, R. Celella, *Il principio di responsabilizzazione: la novità del GDPR,* in *Ciberspazio e Diritto,* 60, 2018, 211 ss.

[5] CEDU, *Testimoni di Geova c. Finlandia,* cit., § 6.

[6] Ivi, § 12.

parte integrante delle forme di manifestazione del credo religioso: in questa prospettiva, deve prevalere su ogni altra considerazione quella volta a tutelare la libertà religiosa della Comunità dei Testimoni, con una conseguenza. La Comunità non può essere qualificata ai sensi della legge finlandese sui dati personali come «soggetto titolare del trattamento dei dati»[7]. Quasi superfluo ricordare come anche questa pronuncia non ponga fine alla vicenda; la controversia giunge difatti dinanzi alla Corte amministrativa suprema finlandese, che solleva una questione pregiudiziale di fronte alla Corte di giustizia dell'Unione europea affinché quest'ultima chiarisca la questione alla luce della disciplina sovranazionale[8].

3. La prospettiva della Corte di giustizia

Con la sentenza del 2018[9], la Corte di giustizia dell'Unione europea stabilisce che l'art. 2, lett. d), della direttiva 95/46/CE, così come interpretato alla luce dell'art. 10, par. 1, della Carta dei diritti fondamentali, permette di definire anche una comunità religiosa come responsabile del trattamento di dati personali – anche se questi ultimi sono stati raccolti e poi conservati nell'esercizio di attività di predicazione[10]. In particolare, il rispetto delle norme eurounitarie in materia di protezione dei dati personali non lede l'autonomia organizzativa di una comunità religiosa di cui all'art. 17 TFUE[11]: per la Corte di Lussemburgo, infatti, ogni comunità religiosa può liberamente e sempre organizzare, coordinare e incoraggiare l'attività di proselitismo realizzata dei suoi membri[12]. Nel caso in cui, però, questa attività comporti anche la raccolta e la conservazione – a qualsiasi scopo – di dati, la comunità religiosa si configura necessariamente come titolare del trattamento dei dati così raccolti. A questo scopo non rileva che la comunità religiosa abbia accesso ai dati raccolti in modo autonomo e indipendente dai membri predicatori, o che essa abbia fornito agli stessi indicazioni inerenti al trattamento[13].
Come facilmente intuibile, il Tribunale amministrativo finlandese si è pronunciato in

[7] Ivi, § 32.

[8] Ivi, § 17.

[9] CGUE, C-25/17, *Jehovan todistajat* (2018). La pronuncia è stata commentata da R. Gellert, *Door-to-Door Preaching by Jehovah's Witnesses Community Falls under Data Protection Law*, in *European Data Protection Law Review*, 4, 2018, 391 ss.; F. Danini, *La tutela del dato personale alla prova dell'attività di predicazione religiosa: libertà di proselitismo o diritto alla privacy?* in *DPCE online*, 4, 2018, 1185 ss.; R. Panettta - F. Sartore, *Proselitismo religioso e protezione dei dati personali: tra esigenze di tutela e particolarità della fattispecie*, in *Responsabilità civile e previdenziale*, 1, 2019, 101 ss.; V. D'Antonio, *Predicazione porta a porta, "archivi" di dati personali e tutela della riservatezza*, in *La nuova giurisprudenza civile commentata*, 2, 2019, 319 ss.

[10] Ivi, § 62.

[11] La disposizione è stata ampliamente analizzata e commentata in dottrina. Sul punto sia consentito il rinvio a D. Durisotto, *Unione europea, chiese e organizzazioni filosofiche non confessionali (art. 17 TFUE), in Stato, Chiese e pluralismo confessionale*, 23, 2016, 1 ss.; F. Margiotta Broglio - M. Orlandi, *Articolo 17 TFUE*, in A. Tizzano (a cura di), *Trattati dell'Unione europea*, Milano, 2014, 457 ss.; M. Lugato, *L'Unione europea e le Chiese: l'art. 17 TFUE nella prospettiva del principio di attribuzione, del rispetto delle identità nazionali e della libertà religiosa*, in *Quaderni di diritto e politica ecclesiastica*, 2, 2014, spec. 307.

[12] CGUE, *Jehovan todistajat*, cit., § 75.

[13] Ivi, § 62.

modo conforme a quanto stabilito dalla Corte di Giustizia; i Testimoni di Geova, invece, hanno ritenuto necessario rivolgersi alla Corte di Strasburgo, sostenendo che i Giudici nazionali non hanno individuato il corretto equilibrio fra i due diritti in gioco – la libertà religiosa e il diritto alla vita privata (o, per meglio dire, alla tutela delle persone fisiche con riguardo al trattamento e alla circolazione dei dati personali).

4. La decisione della Corte europea dei diritti dell'uomo

La giurisprudenza della Corte europea dei diritti dell'uomo ha posto la libertà di pensiero, di coscienza e di religione a fondamento di ogni società democratica[14]. La previsione di cui all'art. 9 CEDU ha vitale importanza non soltanto per ogni credente, ma anche – e come ovvio – per gli atei, gli agnostici, gli scettici e addirittura per chi è indifferente rispetto al fenomeno religioso. L'art. 9 CEDU, ossia la poliedrica libertà che esso tutela, esprime infatti quel particolare ampio pluralismo che è imprescindibile corollario di ogni comunità democratica («indissociabile», nelle parole della Corte EDU)[15]. Proprio nel caso in esame, e nonostante il consolidato orientamento giurisprudenziale volto a tutelare nel contesto appena accennato la libertà religiosa, i Giudici di Strasburgo adottano però una chiave di interpretazione della vicenda finlandese che fa riflettere, tanto rischia di incidere, al fondo, sulla libertà religiosa di alcune particolari congregazioni.

Per la Corte EDU, i predicatori non hanno chiaramente richiesto e ottenuto il consenso espresso, da parte delle persone da loro contattate, alla raccolta, alla conservazione e al successivo trattamento dei loro dati. Anche se questa modalità di raccolta aveva quale fine solo quello di non ricontattare persone disinteressate ad approfondire il credo dei Testimoni, la mancanza del consenso esplicito costituisce una violazione della tutela delle persone fisiche con riguardo al trattamento e alla circolazione dei dati personali – e, di conseguenza, del diritto al rispetto alla vita privata[16]. Al di là dell'ovvio, c'è da chiedersi per quale motivo la Corte EDU adotti una posizione così netta.

Molteplici sono i profili richiamati dai giudici in vari passaggi della sentenza, merita però particolare attenzione sottolineare un aspetto che, a giudizio di chi scrive, è centrale nell'analisi che si sta conducendo: i Giudici di Strasburgo ritengono che la libertà di religione dei Testimoni non venga lesa in alcun modo. La disciplina posta a tutela dei dati personali e del diritto al rispetto alla vita privata, infatti, per la Corte non persegue lo scopo di ingerire nelle attività di proselitismo di una confessione religiosa; al contrario, essa è mirata soltanto a garantire il diritto all'autodeterminazione informativa[17]. Inoltre, continuano i Giudici di Strasburgo, anche laddove la garanzia di quest'ultimo diritto finisse col limitare la libertà religiosa, questa conseguenza andrebbe ricondotta a un quadro specifico. All'interno di una società democratica, la riserva di legge – fra molto altro – garantisce che un diritto di libertà possa essere compresso senza correre

[14] *Ex multis* CEDU, Grande Camera, *Dudgeon c. Regno Unito*, ric. 7525/76 (1981), § 54.

[15] CEDU, *Testimoni di Geova c. Finlandia*, cit., § 72.

[16] Ivi, § 95

[17] Ivi, § 79.

il rischio di essere eliso, proprio quando ciò si rende necessario per garantire l'esercizio e la protezione di altri diritti e libertà. Nel caso di specie, peraltro, obbligare una comunità religiosa a rispettare la disciplina sui dati configura unicamente una forma di tutela adeguata a impedire qualsiasi divulgazione di dati personali in contrasto con le garanzie di cui all'art. 8 CEDU[18]. La qualificazione della Comunità dei Testimoni di Geova come titolare del trattamento dei dati non comporta quindi alcuna forma e alcuna limitazione della attività di proselitismo che, per la stessa congregazione, è parte integrante del credo: tutto al contrario, proprio quella qualificazione riesce a porre in equilibrio la libertà di religione da un lato, e il rispetto alla vita privata dall'altro[19].

5. Considerazioni conclusive

Come anticipato, questa soluzione giurisprudenziale – apprezzabile per l'intento – impone alcune riflessioni critiche. Non v'è dubbio alcuno che gli artt. 8 e 9 CEDU debbano essere interpretati tenendo in particolare considerazione la vigente disciplina sulla protezione dei dati personali[20] e nessun dubbio è presente sulla imprescindibile difficoltà dei Giudici sul bilanciamento dei diritti richiamati dalle singole disposizioni. Data tale premessa, sembra che la Corte EDU, nell'affrontare il caso finlandese, abbia perso un'occasione per definire in modo più problematico il bilanciamento fra tutela dei dati personali e libertà di religione.

Come mette bene in evidenza il caso specifico dei Testimoni di Geova, la libertà religiosa è un diritto estremamente complesso. Quando viene espresso attraverso attività di proselitismo[21], esso viene esercitato dai singoli membri di una congregazione anzitutto sviluppando un rapporto umano con i possibili credenti. Che una simile relazione debba sottostare a formalità quali la manifestazione esplicita del consenso al trattamento di dati è cosa che – di conseguenza e nella migliore delle ipotesi – dovrebbe quantomeno passare attraverso valutazioni che la Corte non ha svolto. La sentenza non chiarisce se vi è differenza fra la protezione da garantire a ogni dato raccolto e conservato, oppure specificamente a una determinata categoria di dati aventi una specifica natura[22] ; non approfondisce inoltre se l'imposizione di simili formalità nel caso di specie si risolva *di fatto* in un ostacolo che scoraggia l'attività di proselitismo al punto da impedirla; non si sofferma, poi, sulla delicatezza del rapporto umano sopra accennato, premessa indispensabile di ogni esercizio di predicazione; sembra, infine, dimenticare che i Testimoni non sono paragonabili ad altri soggetti (pubblici o privati) che, in ragione delle loro attività, sono titolari di trattamento[23].

[18] Ivi, § 102.

[19] Ivi, § 94.

[20] F. Balsamo, *La protezione dei dati personali di natura religiosa*, Cosenza, 2022.

[21] D. Durisotto, *La libertà religiosa individuale. Contenuti e problematiche*, in C. Cardia (a cura di), *Diritto e religione in Italia. Principi e temi*, Roma, 2021, 57-58.

[22] A. Arena, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quaderni costituzionali*, 3, 2014, 722 ss.

[23] M. Bassini, *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quaderni*

È solo adottando questo approccio, però, che la Corte può giungere a ritenere che l'obbligo imposto alla Comunità sia necessario «una società democratica»[24], e che le autorità nazionali abbiano ben bilanciato i diritti in rilievo.
Purtroppo, in questa luce pare possibile sostenere che la Corte EDU abbia perso una vera e propria occasione per riflettere in modo rinnovato sulla libertà religiosa grazie alla non facile questione del suo bilanciamento con il diritto alla protezione dei dati personali.

costituzionali, 3, 2016, 589 ss.

[24] CEDU, *Testimoni di Geova c. Finlandia*, cit., § 98.

La sentenza n. 170 del 2023: la Corte costituzionale chiarisce il perimetro della nozione di corrispondenza e torna sull'interpretazione della legge n. 140 del 2003*

Pietro Villaschi

Corte costituzionale, 27 luglio 2023, n. 170

Analogamente all'art. 15 Cost., quanto alla corrispondenza della generalità dei cittadini, anche, e a maggior ragione, l'art. 68, c. 3, Cost. tutela la corrispondenza dei membri del Parlamento – ivi compresa quella elettronica – anche dopo la ricezione da parte del destinatario, almeno fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento "storico".

Sommario

Keywords

sequestro di corrispondenza - comunicazioni telematiche - guarentigie parlamentari - posta elettronica - WhatsApp

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

1. Introduzione: il caso oggetto del conflitto di attribuzione sollevato dal Senato

Con la sentenza n. 170 del 2023 la Corte costituzionale ha deciso il conflitto di attribuzione tra poteri dello Stato promosso dal Senato della Repubblica nei confronti della Procura della Repubblica di Firenze, a seguito dell'acquisizione da parte di quest'ultima di plurime comunicazioni del senatore Matteo Renzi nell'ambito di un procedimento penale a suo carico[1].

Oggetto dell'indagine era, nello specifico, il sostegno economico prestato dalla Fondazione Open all'attività politica del senatore Renzi (e della relativa corrente del Partito democratico), che, ad avviso degli inquirenti, avrebbe configurato un'ipotesi di finanziamento illecito. All'esito dell'attività investigativa la Procura aveva sottoposto a sequestro probatorio i telefoni cellulari di due degli indagati, Vittorio Ugo Manes e Marco Carrai, nella cui memoria erano conservati una serie di messaggi intercorsi con il senatore Renzi sia a mezzo WhatsApp (nei giorni 3-4 giugno 2018 e dal 12 agosto 2018 al 15 ottobre 2019) che per posta elettronica (dal 1° agosto 2018 al 10 agosto 2018). Contestualmente gli inquirenti avevano sequestrato l'estratto del conto corrente bancario del senatore riferito al periodo dal 14 giugno 2018 al 13 marzo 2020.

Con delibera assunta alla seduta del 22 febbraio 2022[2], il Senato aveva sollevato ricorso per conflitto tra poteri dello Stato, assumendo che la Procura avesse leso le proprie attribuzioni costituzionali, avendo acquisito la corrispondenza di un membro del Parlamento in assenza della necessaria autorizzazione preventiva della Camera di appartenenza, richiesta dall'art. 68, c. 3, Cost.

La Corte costituzionale, nell'accogliere il ricorso - fatta eccezione, come si vedrà oltre (par. n. 2.3), per la sola ipotesi dell'acquisizione dell'estratto del conto corrente del senatore - segna un precedente di indubbio rilievo, destinato ad avere riflessi ben al di là dei confini del caso da cui era originato il conflitto[3].

La motivazione si può dividere in due parti fondamentali.

Nella prima (nn. 4-4.1-4.2-4.3-4.4-4.5 del Considerato in diritto) il Giudice delle Leggi risolve la questione di fondo all'origine del ricorso, chiarendo il perimetro della nozione di corrispondenza ed estendendola alle comunicazioni di natura telematica, anche qualora queste siano già state recapitate e siano conservate nella memoria del dispositivo del destinatario. Trattasi di una presa di posizione che, smentendo un consolidato orientamento della giurisprudenza di legittimità, travalica il tema dei confini della tutela delle comunicazioni dei parlamentari ed è preordinata a dispiegare i suoi effetti

[1] Ricorso per conflitto di attribuzione tra poteri dello Stato n. 10 del 2022, promosso dal Senato della Repubblica nei confronti della Procura della Repubblica di Firenze, pubblicato su G.U. 1a Serie Speciale - Corte Costituzionale n. 3 del 18.01.2023.

[2] Cfr. resoconto stenografico della seduta pubblica del Senato n. 406 del 22.02.2022, nella quale l'Assemblea approvava la relazione della Giunta delle elezioni e delle immunità parlamentari del 14 dicembre 2021, comunicata alla Presidenza del Senato il 20 dicembre 2021 (Doc. XVI n. 9).

[3] Per un primo commento alla pronuncia, cfr. G. Guzzetta, *La nozione di comunicazione e altre importanti precisazioni della Corte costituzionale sull'art. 15 della Costituzione nella sentenza n. 170 del 2023,* in *Federalismi*, 21, 2023, 81 ss.; M. Borgobello, *Il concetto di "corrispondenza" nella sentenza 170 del 2023 della Corte costituzionale*, in *Giurisprudenzapenaleweb*, 8, 2023, 1 ss.

a garanzia della generalità dei consociati, consentendo l'applicazione delle guarentigie costituzionali in materia di corrispondenza ai mezzi di comunicazione oggi più diffusi, ossia i messaggi *WhatsApp* e la posta elettronica (nonché, più in generale, le diverse forme di comunicazione elettronica).
Nella seconda (nn. 5-5.1-5.2 del Considerato in Diritto) la Corte chiarisce, invece, una questione interpretativa particolarmente complessa, data anche l'assenza di precedenti in materia, relativa al modulo procedurale applicabile alle ipotesi di sequestro di corrispondenza di un parlamentare ai sensi dell'art. 68, c. 3, Cost. e della l. 140/2003, con particolare riferimento al caso in cui a essere posto sotto sequestro sia il dispositivo di un terzo. Come si vedrà, la soluzione offerta, discostandosi dalla tradizionale distinzione tra attività investigativa diretta/mirata, da una parte, e casuale, dall'altra, elaborata dalla Corte con riferimento alle intercettazioni di conversazioni e comunicazioni e all'acquisizione dei tabulati telefonici[4], apre una serie di spunti di riflessione di sicuro interesse.

2. Le nozioni di corrispondenza a confronto: le tesi del Senato e della Procura

La questione di fondo su cui la Corte costituzionale era stata chiamata a interrogarsi concerneva, come anticipato, il perimetro applicativo della nozione di corrispondenza ai sensi degli artt. 15 e 68, c. 3, Cost. Si trattava di una questione di particolare delicatezza, stante l'assenza, da un lato, di precedenti inerenti l'interpretazione dell'art. 15 Cost. che avessero avuto ad oggetto specificamente comunicazioni di carattere telematico (che, per ovvie ragioni storiche, la Costituzione non prende direttamente in considerazione), e, dall'altro, per il fatto che la pur copiosa giurisprudenza costituzionale sull'art. 68, c. 3, Cost. mai aveva avuto prima ad oggetto ipotesi di sequestro di corrispondenza (nemmeno epistolare) di parlamentari, ma esclusivamente casi di intercettazioni di natura telefonica oppure di acquisizione di tabulati telefonici.
Preliminarmente, si ritiene allora utile precisare quali siano, ad avviso della dottrina maggioritaria[5], i caratteri tipici della nozione di corrispondenza, identificabili nella segretezza, nell'inter-subiettività e nell'attualità della comunicazione. Una sintetica rico-

[4] Cfr., in particolare, Corte cost., 6 marzo 2019, n. 38; Corte cost., 28 maggio 2010, n. 188, Corte cost., 25 marzo 2010, n. 114, Corte cost., 25 marzo 2010, n. 113; Corte cost., 23 novembre 2007, n. 390.

[5] In materia cfr. P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, 163 ss.; P. Barile-E. Cheli, *Corrispondenza (libertà di)*, in *Enc. Dir.*, X, Milano, 1962, 743 ss.; P. Caretti, *I diritti fondamentali*, Torino, 2005, 275 ss.; P. Caretti, *Diritto dell'informazione e della comunicazione: stampa, radiotelevisione, telecomunicazioni, teatro e cinema*, Bologna, 2005; P. Caretti, *Corrispondenza (libertà di)*, in *Digesto pubbl.*, IV, Torino, 1989, 200 ss.; M. Cuniberti (a cura di), *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici*, Milano, 2008; F. Donati, *Art. 15*, in R. Bifulco-A. Celotto-M. Olivetti (a cura di), *Commentario alla Costituzione*, vol. 1, Torino, 2006, 362 ss.; M. Di Majo, *Corrispondenza (dir. priv.)*, in *Enc. Dir.*, XI, Milano, 1962, 741 ss.; A. Pace, *Art. 15*, in *Comm. Cost. Branca*, Bologna-Roma, 1977, 80 ss.; A. Pace, *Problematica delle libertà costituzionali. II. Parte speciale*, Padova, 1992; Id., *Contenuto e oggetto della libertà di corrispondenza e di comunicazione*, in *Scritti in onore di C. Mortati*, I, Milano, 1977, 813 ss.; G.M. Salerno, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in R. Nania - P. Ridola (a cura di), *I Diritti costituzionali*, Torino, I, 2001, 417 ss.; A. Valastro, *Libertà di comunicazione e nuove tecnologie*, Milano, 2001; R. Zaccaria, *Diritto dell'informazione e della comunicazione*, Padova, 2004.

struzione al riguardo è, infatti, necessaria, stante il fatto che la (condivisibile) soluzione cui approda la Corte costituzionale si fonda proprio su una rilettura di tali requisiti - e di quello dell'attualità in particolare - originariamente formulati con riferimento alla corrispondenza epistolare.

Quanto al primo carattere, quello della segretezza, la dottrina concorda sul fatto che sussista uno stretto legame tra segretezza e libertà della corrispondenza[6]. Secondo un orientamento, l'art. 15 Cost. tutelerebbe, infatti, «una sola situazione giuridica soggettiva: la libertà delle comunicazioni materialmente assoggettabili e concretamente assoggettate a vincolo di segretezza»[7], cessando, quindi, di operare automaticamente alla presa visione da parte del destinatario. Secondo altro filone, pur sussistendo un chiaro legame, "libertà" e "segretezza" costituirebbero due distinte situazioni soggettive. Si dovrebbe quindi derivare la conclusione che, quand'anche il mittente abbia scelto uno strumento di comunicazione "aperto", la garanzia costituzionale possa tornare a dispiegarsi dal momento della ricezione da parte del destinatario della comunicazione, qualora quest'ultimo abbia interesse a mantenerne riservato il contenuto[8].

Con "inter-subiettività" si intende, invece, la necessità che un messaggio sia destinato ad uno o più soggetti determinati. Secondo l'orientamento prevalente, a tal fine, sarebbe decisivo l'animus del mittente e, invece, irrilevante sia il contenuto trasmesso, sia la forma adoperata, sia, infine, lo strumento di trasmissione[9]; ad avviso di una tesi più restrittiva, al contrario, la tutela offerta dalla disposizione costituzionale in oggetto riguarderebbe le sole comunicazioni di pensiero generalmente riconoscibili come tali[10].

Decisivo, infine, il terzo requisito, il più controverso, ossia l'attualità della comunicazione, che cessa di essere tale quando, per il decorso del tempo, ne viene meno il carattere privato e personale ed il suo oggetto acquista un mero valore retrospettivo, affettivo, collezionistico, storico, artistico, scientifico o probativo. Secondo una tesi più "estensiva", siffatto momento potrebbe essere anche successivo all'apertura della missiva da parte del destinatario e la sua individuazione richiederebbe, pertanto, un'indagine volta a tenere conto, caso per caso, del valore della comunicazione e dell'intenzione di mittente e destinatario di considerarla ancora attuale[11]; secondo un diverso

[6] Cfr. P. Barile, *Diritti dell'uomo*, cit., 163, che osserva come la corrispondenza «è libera in quanto segreta ed è al contempo segreta per poter essere libera». Sul punto, si veda, altresì, Corte cost., 26 gennaio 2017, n. 20, Considerato in Diritto n. 3.1., che nel riprendere la sent. 23 luglio 1991, n. 366 ricorda che: «La "libertà" e la "segretezza" della «corrispondenza e di ogni altra forma di comunicazione» sono oggetto del diritto «inviolabile» tutelato dall'art. 15 Cost., che garantisce «quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana».

[7] Cfr. A. Pace, *art. 15*, cit., 85.

[8] Cfr. P. Barile, *Diritti dell'uomo*, cit., 164; M. Petrone, *voce Segreti (delitti contro l'inviolabilità dei)*, in *Noviss. Dig. It.*, XVI, Torino, 1969, 972.

[9] P. Barile-E. Cheli, *Corrispondenza (libertà di)*, cit., 744-745; inoltre, v. P. Barile, *Diritti dell'uomo*, cit., 164-165.

[10] In questi termini, la busta suggellata sarebbe, quindi, tutelata dall'art. 15 Cost., ma non, ad esempio, un pacco, che secondo i criteri di generale riconoscibilità non sarebbe riconosciuto come strumento idoneo a veicolare un pensiero da un individuo ad un altro, cfr. A. Pace, *art. 15*, cit., 81-82.

[11] Cfr., in particolare, P. Barile, *Diritti dell'uomo*, cit., 164-165, che rileva come per «corrispondenza si intende quella epistolare, telegrafica, telefonica, con collegamento tramite filo o "ad onde guidate" […]. Il concetto abbraccia in verità ogni possibile corrispondenza: si pensi ad esempio ai segnali ottici da punto a punto, ai segnali acustici (tamburi nella giungla, e meno romanticamente, "radio-carcere"

orientamento, invece, l'attualità verrebbe meno automaticamente nel momento in cui il messaggio sia stato recapitato e visionato dal destinatario[12].

In questa complessa cornice teorica si inserisce il caso sottoposto all'attenzione della Corte costituzionale.

Ad avviso del Senato la nozione di corrispondenza si presterebbe a includere non solo la tradizionale corrispondenza epistolare cartacea, ma anche quella di carattere telematico. Quest'ultima sarebbe, infatti, assistita dalle medesime garanzie di segretezza, di cui si diceva poc'anzi, assicurate in particolare da credenziali di accesso riservate e dalla disponibilità esclusiva, in capo ai corrispondenti, dei dispositivi elettronici utilizzati per lo scambio dei messaggi. In secondo luogo, anche con riferimento alle comunicazioni telematiche sussisterebbe il requisito dell'attualità, che si estenderebbe ai messaggi recapitati e conservati sulla memoria del destinatario, elemento questo di particolare importanza dato che, in tali forme di comunicazione, per ragioni tecniche, all'invio segue immediatamente il recapito. Questione, tuttavia, tutt'altro che di agevole soluzione. Un consolidato orientamento della giurisprudenza di legittimità[13], richiamato non a caso dalla Procura a fondamento delle proprie difese, era, infatti, costante nell'affermare che i messaggi come *SMS*, *WhatsApp* o *e-mail*, cesserebbero di essere "corrispondenza" una volta recapitati sul dispositivo del destinatario, ma dovrebbero essere, al contrario, considerati come meri "documenti", sicché sarebbe legittima la loro libera acquisizione nel procedimento mediante riproduzione fotografica ai sensi dell'art. 234 c.p.p., non trovando applicazione né le garanzie previste per le intercettazioni *ex* art. 266 ss. c.p.p., né quelle relative al sequestro di corrispondenza di cui all'art. 254 c.p.p. In altri termini, ad avviso della Procura, le guarentigie di cui agli artt. 15 e 68, c. 3, Cost. si interromperebbero per effetto del mero recapito del messaggio, non estendendosi alla "dimensione statica" della comunicazione.

Un discorso a parte merita la qualificazione dell'estratto del conto corrente bancario del senatore acquisito dagli inquirenti. Ad avviso del Senato sarebbe, infatti, inequivocabile la sussunzione sotto la nozione di corrispondenza dell'estratto conto, che altro non sarebbe che una comunicazione che la banca invia al cliente contenente dati riservati, quali le operazioni di dare e di avere compiute in un determinato periodo, con indicazione dei destinatari e delle causali. Opposta la tesi della Procura, secondo la quale, invece, si tratterebbe di un documento che non nasce per essere trasmesso,

mediante il tambureggiamento sui muri da cella a cella). Questo tipo di comunicazioni hanno dunque un carattere intersoggettivo (fra soggetti determinati) e hanno anche, per loro natura, un carattere attuale: diventano corrispondenza nell'atto in cui viene scelto e utilizzato il mezzo di trasmissione (la lettere non è tale prima di essere imbucata), cessano di essere tale non, come alcuni sostengono, all'atto del ricevimento e della presa di conoscenza da parte del destinatario, bensì quando per decorso del tempo ha trasformato il messaggio in un documento storico, avente carattere meramente retrospettivo (mancanza dell'attualità)»; ed anche F. Antolisei, *Manuale di Diritto penale*, Milano, 2003, 253, che ritiene che la corrispondenza perda, caso per caso, il suo carattere di attualità - divenendo un semplice documento - «quando, per decorso del tempo od altra causa, non le si può assegnare che un valore meramente retrospettivo, affettivo, collezionistico, storico, artistico, scientifico o probatorio».

[12] Cfr. A. Pace, *art. 15,* cit., 90; V. Italia, *Libertà e segretezza della corrispondenza e delle comunicazioni*, Milano, 1963, 212; C. Troisio, *Corrispondenza, libertà e segretezza della corrispondenza*, in *EG*, IX, Roma, 1988, 10.

[13] Tra le ultime, Cass. pen., sez. II, 19 ottobre 2022, n. 39529, in *Quotidiano Giuridico*, 2022; Cass. pen., sez. VI, 8 giugno 2022, n. 22417; Cass. pen., sez. V, 6 maggio 2021, n. 17552, in *Quotidiano Giuridico*, 2021.

pur potendolo essere, ma che ha la funzione di riepilogo di operazioni dispositive in entrata o in uscita. A ragionare diversamente, ad avviso della resistente, si dovrebbe, difatti, pervenire alla paradossale conclusione che l'acquisizione di qualsiasi scritto, semplicemente perché inserito all'interno di un plico, resterebbe sottoposta alle regole sul sequestro di corrispondenza anche una volta conclusa la spedizione.

2.1. La soluzione offerta dalla Corte costituzionale: le comunicazioni di natura elettronica, purché riservate, costituiscono "corrispondenza" a tutti gli effetti

La Corte costituzionale, con motivazione ampia, approfondita e pienamente condivisibile[14], sposando la tesi del Senato, qualifica come corrispondenza i messaggi *WhatsApp* e di posta elettronica anche (e soprattutto) nella loro dimensione prettamente "statica". Si tratta di una presa di posizione importante e non scontata, anche in considerazione del fatto che, come si è visto poc'anzi retro (par. n. 2), la giurisprudenza di legittimità militava in senso diametralmente opposto.

La prima pietra su cui si regge il ragionamento del giudice costituzionale concerne una distinzione preliminare e fondamentale, ossia quella tra intercettazione di conversazioni o comunicazioni, da una parte, e sequestro di corrispondenza, dall'altra. In dottrina, come in giurisprudenza, erano state, infatti, formulate diverse tesi al riguardo[15]. Il Giudice delle Leggi, rigettando le posizioni sia del Senato che della Procura - che avevano sostenuto che si sarebbe in presenza di un'intercettazione solo nel caso di una comunicazione orale e, invece, di un sequestro di corrispondenza in caso di acquisizione di

[14] In merito alla necessità che la Corte, alla luce dell'evoluzione delle nuove forme di comunicazione telematica, qualificasse, senza ambiguità, la posta elettronica e i messaggi *WhatsApp* come corrispondenza, sia consentito rinviare a P. Villaschi, *La posta elettronica e i messaggi WhatsApp sono corrispondenza? Note a margine del ricorso per conflitto di attribuzione tra poteri dello Stato promosso dal Senato della Repubblica in relazione al "caso Renzi"*, in *Federalismi*, 7, 2023, 234 ss.; cfr. altresì E. Albanesi, *Messaggistica WhatsApp ed e-mail nel contesto delle prerogative dei membri del Parlamento ex art. 68, terzo comma, Cost. Prospettive costituzionali di diritto della comunicazione*, in questa *Rivista*, 3, 2022, 94 ss.

[15] Secondo un primo orientamento, il criterio distintivo tra intercettazione di conversazioni e sequestro di corrispondenza sarebbe stato quello "temporale": in caso di captazione in tempo reale di un flusso comunicativo in fieri, avrebbe operato la disciplina delle intercettazioni; viceversa, i messaggi già recapitati e archiviati sul dispositivo del destinatario, in quanto costituenti un flusso concluso, non sarebbero stati ricompresi nel materiale intercettabile ma in quello sequestrabile, cfr. A. Aprile, *Intercettazioni di comunicazioni*, in A. Scalfati (a cura di), *Prove e misure cautelari*, in *Trattato di procedura penale*, diretto da G. Spangher, II, cit., 535; L. Luparia, *Computer crimes e procedimento penale*, in G. Garuti (a cura di), *Modelli differenziati di accertamento*, in *Trattato di procedura penale*, diretto da G. Spangher, VII, I, Torino, 2011, 387; A. Vele, *Documento informatico e tutela della riservatezza nel processo penale: aspetti problematici,* in *Archivio Penale*, 1, 2018; secondo altro filone, decisive sarebbero state le "modalità di esecuzione" dell'atto di indagine: si sarebbe trattato di intercettazione, quindi, quando l'attività di captazione fosse stata effettuata a distanza ed in modo occulto; di sequestro, qualora l'atto investigativo, seppur a sorpresa, fosse stato eseguito in modo palese. Inoltre, se lo scopo fosse stato quello di privare il titolare della disponibilità materiale del messaggio, le norme che si sarebbero applicate sarebbero state quelle sul sequestro di corrispondenza (artt. 254, 254-bis e 352 c.p.p.); se, viceversa, l'obiettivo fosse stato quello di apprendere, in modo occulto, un flusso comunicativo in corso, si sarebbe dovuto fare ricorso all'intercettazione telematica *ex* art. 266 ss. c.p.p., cfr. F. Zacché, *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. giust.*, 4, 2013, 106; M. Pittituti, *Profili processuali della prova informatica*, in L. Marafioti-G. Paolozzi (a cura di), *Incontri ravvicinati con la prova penale. Un anno di seminari a Roma Tre*, Torino, 2014, 59.

una comunicazione scritta - ritiene che la linea di confine tra le due nozioni si trovi altrove. In particolare, affinché si possa parlare di intercettazione occorre, ad avviso della Corte, che siano verificate due condizioni: anzitutto, che la comunicazione sia in corso di svolgimento e, quindi, captata nel suo momento "dinamico"; al contrario, in caso di acquisizione del supporto fisico che reca memoria di una comunicazione già avvenuta - dunque, nel suo momento "statico" - si rientra nel sequestro di corrispondenza; in secondo luogo, perché si tratti di intercettazione è necessaria l'apprensione del messaggio comunicativo in modo occulto, ossia all'insaputa dei soggetti tra i quali la comunicazione intercorre[16].

Trattasi di una soluzione condivisibile, in coerenza peraltro con alcuni importanti approdi della giurisprudenza di legittimità, che forse avrebbero potuto essere maggiormente valorizzati nel corpo della motivazione[17]. Conseguenza pratica di tale impostazione, che rifugge quindi la schematica distinzione tra comunicazione orale e scritta, è che, in caso di flusso di comunicazioni telematiche in corso (per esempio *e-mail* o *fax*) si potrà procedere ad intercettazione (per quanto si tratti di messaggi scritti)[18], nell'ipotesi, invece, di un messaggio audio via *WhatsApp* si rientrerà nel perimetro della nozione di corrispondenza (per quanto la comunicazione sia orale).

Ad ogni modo, appare chiaro il motivo per il quale il Giudice delle Leggi affronta tale profilo in via preliminare. La distinzione tra intercettazione di conversazioni e sequestro di corrispondenza è infatti fondamentale ai fini della risoluzione del conflitto, dal momento che, per quanto l'art. 68, c. 3, Cost. richieda genericamente, in entrambe le ipotesi, l'autorizzazione della Camera di appartenenza, ad essere differente (come si avrà modo di illustrare infra, par. n. 3) è il modulo procedurale applicabile alle due fattispecie ai sensi della l. 140/2003, specie nel caso in in cui ad essere posto sotto sequestro è il dispositivo di terze persone e non direttamente quello del parlamentare.

Tanto premesso, nel caso oggetto del conflitto, non si rientrava chiaramente nell'ipotesi di un'intercettazione, dal momento che l'acquisizione delle comunicazioni del senatore Renzi era avvenuta da parte degli inquirenti a conversazioni concluse e in modo palese.

Chiariti i confini tra le due nozioni, la Corte può così entrare ad affrontare il cuore della questione giuridica sottopostale, sposando la tesi sostenuta dalla difesa del Senato e arricchendola di ulteriori argomentazioni. La motivazione si struttura in due parti fondamentali.

Nella prima (n. 4.2 del Considerato in diritto) il giudice costituzionale chiarisce come, nonostante i messaggi *WhatsApp* e le *e-mail* non siano espressamente qualificati dall'ordinamento come corrispondenza, più indici depongano, senza dubbio, in tale direzione. Nella seconda (nn. 4.3-4.4 del Considerato in diritto) precisa che la nozione di corrispondenza si estende anche alle comunicazioni elettroniche nella loro dimensio-

[16] Corte cost., 27 luglio 2023, n. 170, Considerato in diritto n. 4.1.

[17] Ad esempio, chiarissima, in questo senso, peraltro con riferimento proprio a conversazioni di natura telematica, era stata la pronuncia della Cass pen., sez. V, 4 novembre 2020, n. 30735, che aveva escluso dall'ambito di applicazione dell'art. 616 c.p., la presa visione delle *e-mail*, qualora la loro trasmissione fosse in corso, in quanto la norma incriminatrice considererebbe la "corrispondenza" in senso esclusivamente statico; su questi aspetti, più nello specifico, infra par. n. 2.2.

[18] Cfr., sul punto, E. Aprile-F. Spiezia, *Le intercettazioni telefoniche ed ambientali*, Milano, 2004.

ne statica, ossia qualora il messaggio sia stato già recapitato e risulti conservato nella memoria del dispositivo del destinatario.

Muovendo dalla prima parte della motivazione, la Corte rileva a sostegno dell'assimilazione delle comunicazioni di natura telematica alla nozione di corrispondenza quanto segue.

Preliminarmente, ricorda che la nozione di corrispondenza *ex* art. 15 Cost. è, tradizionalmente, stata intesa in senso piuttosto ampio ad abbracciare «ogni comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate»[19], che non siano in presenza.

In secondo luogo, osserva che tale qualificazione prescinde dalle caratteristiche tecniche del mezzo tecnico utilizzato ai fini del pensiero. È questo uno dei passaggi sicuramente più significativi della pronuncia. La Corte richiama, infatti, importanti precedenti, coi quali aveva fornito un'interpretazione estensiva delle guarentigie costituzionali in commento. Tra le pronunce evocate spiccano la sentenza n. 1030 del 1988, nella quale, con riferimento agli apparecchi ricetrasmittenti di debole potenza, la Corte aveva osservato che «si tratta di strumenti tipicamente preordinati a realizzare comunicazioni interpersonali e non a diffondere messaggi alla generalità (...). Il favor legislativo è, d'altra parte, coerente con la tendenziale espansione delle possibilità di comunicazione implicita nella garanzia costituzionale di cui all'art. 15»[20]; la sentenza n. 81 del 1993, ove la Corte, in un momento in cui internet non era ancora diffuso, aveva affermato che «il riconoscimento e la garanzia costituzionale della libertà e della segretezza della comunicazione comportano l'assicurazione che il soggetto titolare del corrispondente diritto possa liberamente scegliere il mezzo di corrispondenza, anche in rapporto ai diversi requisiti di riservatezza che questo assicura sia sotto il profilo tecnico, sia sotto quello giuridico»[21]; più recenti, sono invece, la sentenza n. 20 del 2017, nella quale il Giudice delle Leggi chiariva che «il diritto di cui all'art. 15 Cost. comprende tanto la «corrispondenza» quanto le «altre forme di comunicazione», incluse quelle «telefoniche, elettroniche, informatiche, tra presenti o effettuate con gli altri mezzi resi disponibili dallo sviluppo della tecnologia»[22] e, da ultimo, la sentenza n. 2 del 2023, ove si valorizzava la circostanza che l'art. 15 Cost. aprisse «il testo costituzionale alla possibile emersione di nuovi mezzi e forme della comunicazione riservata»[23]. Alla luce di tali precedenti, la Corte non può che concludere che «posta elettronica e messaggi inviati tramite l'applicazione WhatsApp (appartenente ai sistemi di cosiddetta messaggistica istantanea)

[19] Corte cost., 27 luglio 2023, n. 170, Considerato in diritto n. 4.2.

[20] Corte cost., 15 novembre 1988, n. 1030, Considerato in diritto n. 8, con nota di R. Niro, *I ponti radio: mezzi di "comunicazione" o mezzi di "trasporto" di programmi destinati alla radiodiffusione?*, in *Giurisprudenza costituzionale*, 10, 1988, parte I, sez. I, 500.

[21] Corte cost., 11 marzo 2023, n. 81, Considerato n. 4, con nota di A. Pace, *Nuove frontiere della libertà di "comunicare riservatamente" (o, piuttosto, del diritto alla riservatezza)*?, in *Giurisprudenza costituzionale*, 1993, 742 ss.

[22] Corte cost., 26 gennaio 2017, n. 20, Considerato in Diritto n. 3.3, con commento di M. Ruotolo, *Regolazione dei mezzi di ricerca della prova e limiti del sindacato della Corte costituzionale (sentenza n. 20 del 2017)*, in *Quaderni costituzionali*, 2, 2017, 376 ss.

[23] Corte cost., 12 gennaio 2023, n. 2, Considerato in Diritto n. 9, con nota di F. Losurdo, *Nucleo essenziale della libertà di comunicazione e riserva di giurisdizione. Esiste un "diritto al mezzo" ?*, in *Giurisprudenza costituzionale*, 1, 2023, 18 ss.

rientrano, dunque, a pieno titolo nella sfera di protezione dell'art. 15 Cost., apparendo del tutto assimilabili a lettere o biglietti chiusi»[24].

La segretezza della comunicazione (retro par. n. 2) torna qui in rilievo. Se, infatti, irrilevanti sono le caratteristiche tecniche del mezzo prescelto per le ragioni anzidette, determinante, affinché si possa parlare di corrispondenza, è, invece, che la comunicazione tra mittente e destinatario sia riservata. Tale segretezza è garantita, per la corrispondenza epistolare-cartacea, dalla chiusura in una busta del testo scritto e, per quella elettronica, dalla visibilità esclusiva del messaggio da parte dei soggetti legittimati ad avere accesso al sistema informatico (tramite, ad esempio, Pin o password). Sul punto, con riferimento specifico proprio alla posta elettronica, si era già espressa la giurisprudenza di legittimità, rilevando che «tale corrispondenza può essere qualificata come "chiusa" solo nei confronti dei soggetti che non siano legittimati all'accesso ai sistemi informatici di invio o di ricezione dei singoli messaggi»[25].

Chiarito, quindi, il perimetro applicativo dell'art. 15 Cost., la Corte cala la riflessione sull'art. 68, c. 3, Cost. dal momento che quest'ultima era la disposizione costituzionale che veniva in rilievo nel conflitto. Sotto questo punto di vista occorreva in particolare chiarire se la mancanza di un riferimento al concetto di ogni "altra forma di comunicazione" oltre a quello di "corrispondenza" - presente all'art. 15 Cost. e assente, invece, all'art. 68, c. 3, Cost. - potesse escludere le comunicazioni elettroniche dalla guarentigia parlamentare[26]. In realtà, tale asimmetria non poneva particolari criticità. Difatti, per quanto la portata dell'art. 68, c. 3, Cost. sembri a prima vista essere più ristretta, già solo il concetto di "corrispondenza" è sufficientemente esteso da ricomprendere i messaggi *WhatsApp* e le *e-mail*, proprio in quanto essi consistono nello scambio di un pensiero in modalità riservata tra soggetti determinati.

Di ciò si mostra consapevole la Corte costituzionale, che supera il problema della supposta diversa portata applicativa delle due disposizioni costituzionali. Sul punto, il primo argomento a sostegno della riconducibilità delle comunicazioni telematiche alla nozione di corrispondenza *ex* art. 68, c. 3, Cost. è, in realtà, più di fatto che non giuridico. Rileva, infatti, il giudice costituzionale che, a ragionare diversamente, si svuoterebbe la guarentigia costituzionale posta a tutela dei parlamentari, che continuerebbe ad operare solo formalmente, in quanto limitata ad ipotesi assolutamente minoritarie e residuali (data la marginalità della corrispondenza cartacea nella pratica). Al riguardo, proprio per dimostrare la centralità dei mezzi di comunicazione di natura elettronica nella contemporanea realtà digitale, si sarebbe, forse, potuta valorizzare maggiormente la recente sentenza n. 2 del 2023, con cui la Corte, nel dichiarare l'illegittimità costituzionale dell'art. 3, c. 4, del d.lgs. 159/2011, nella parte in cui includeva i telefoni cellulari tra gli apparati di comunicazione radiotrasmittente di cui il questore può vietare, in tutto o in parte, il possesso o l'utilizzo, per violazione proprio dell'art. 15 Cost., al

[24] Corte cost., 27 luglio 2023, n. 170, Considerato in diritto n. 4.2.

[25] Cass. pen., sez. V., 19 dicembre 2007, n. 47096.

[26] L'art. 15 Cost. recita infatti: «la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili», mentre l'art. 68, c. 3, Cost. statuisce: «Analoga autorizzazione è richiesta per sottoporre i membri del Parlamento ad intercettazioni, in qualsiasi forma, di conversazioni o comunicazioni e a sequestro di corrispondenza».

punto n. 9 del Considerato in Diritto aveva osservato acutamente che «è difficile pensare che il divieto di possesso e uso di un telefono mobile - considerata l'universale diffusione attuale di questo strumento, in ogni ambito della vita lavorativa, familiare e personale - non si traduca in un limite alla libertà di comunicare […]. Da questo punto di vista, il telefono cellulare ha assunto un ruolo non paragonabile a quello degli altri strumenti evocati dai rimettenti. Rivelerebbe, inoltre, un senso d'irrealtà l'obiezione per cui la libertà di comunicare, privata del telefono mobile, ben potrebbe ancora oggi essere soddisfatta attraverso mezzi diversi, come gli apparati di telefonia fissa»[27].

E, verosimilmente, proprio in quanto consapevole del rischio che una motivazione fondata sulla mera rilevanza "pratica" dei messaggi *WhatsApp* e della posta elettronica potesse risultare debole, la Corte tenta di rafforzarla con due ulteriori argomentazioni, entrambe pienamente condivisibili.

Anzitutto, osserva come soccorre nella direzione considerata la giurisprudenza della Corte Europea dei Diritti dell'Uomo, la quale non ha avuto incertezze nel ricondurre le forme di comunicazione telematica sotto il cono di protezione dell'art. 8 CEDU (ove si fa, peraltro, riferimento alla corrispondenza *tout court* alla stregua dell'art. 68 Cost.) La Corte cita qui una serie di precedenti, ove erano venuti in rilievo proprio i messaggi di posta elettronica[28], gli *SMS*[29] e la messaggistica istantanea inviata e ricevuta tramite internet[30], su cui più diffusamente, infra, par. n. 2.2.

In secondo luogo, a sostegno dell'assimilazione delle comunicazioni di natura elettronica alla nozione di corrispondenza di cui all'art. 68, c. 3, Cost., il Giudice delle Leggi adduce un'ulteriore motivazione, ricordando che, a livello di legislazione ordinaria, il quarto comma dell'art. 616 c.p., come sostituito dall'art. 5 della l. 547/1993, già da tempo include espressamente nella nozione di «corrispondenza» - agli effetti delle disposizioni che contemplano i delitti contro l'inviolabilità dei segreti - oltre a quella epistolare, telegrafica e telefonica, anche quella «informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza». La disposizione in parola fornisce, pertanto, un ulteriore argomento utile a sostegno della tesi secondo cui, sin dal 1993, l'ordinamento accoglierebbe una nozione piuttosto lata di corrispondenza: e tra le comunicazioni telematiche, cui fa riferimento il testo di legge, possono essere certamente ricompresi sia i servizi di messaggistica istantanea, che la posta elettronica.

In definitiva, da tutto quanto precede, la Corte giunge alla conclusione secondo cui, a patto che il testo sia inoltrato a una o più persone determinate in modalità riservata (ossia sussista quel carattere di inter-subiettività e segretezza di cui si diceva retro al par. n. 2), anche i messaggi *WhatsApp* e le *e-mail* sono da considerarsi a tutti gli effetti "corrispondenza" ai sensi sia dell'art. 15 Cost. che dell'art. 68, c. 3, Cost.

---

[27] Corte cost., 12 gennaio 2023, n. 2, Considerato in Diritto n. 9.

[28] CEDU, *Bărbulescu c. Romania*, ric. 61496/08 (2016), § 72; CEDU, *Copland c. Regno Unito*, ric. 62617/00 (2007), § 41.

[29] CEDU, *Saber c. Norvegia,* ric. 459/18 (2020), § 48.

[30] CEDU, *Bărbulescu c. Romania*, cit., § 74.

2.2. … e sono "corrispondenza" anche (e soprattutto) qualora recapitate e conservate sul dispositivo del destinatario

Dopo aver chiarito che la nozione di corrispondenza si estende anche a comunicazioni di natura elettronica, pur in assenza di un riferimento espresso in tal senso in Costituzione, la Corte costituzionale doveva esaminare un ulteriore e più controverso profilo, ossia la possibilità di estendere tale nozione (e conseguentemente la protezione offerta dagli artt. 15 e 68, c. 3, Cost.) alla "dimensione statica" della comunicazione, ossia al messaggio già recapitato e conservato sul dispositivo del destinatario.

Nel dare risposta affermativa a tale interrogativo (nn. 4.3-4.4 del Considerato in Diritto), la Corte risolve un'annosa questione, che, come si è anticipato retro al par. n. 2, aveva diviso dottrina e giurisprudenza in merito all'interpretazione del requisito dell'attualità della comunicazione.

La Corte costituzionale sposa l'orientamento, su cui aveva fatto leva la difesa del Senato (sempre retro par. n. 2), secondo cui la tutela di cui alle disposizioni costituzionali in parola - iniziata nel momento in cui l'espressione del pensiero è affidata ad un mezzo idoneo a trasmetterlo, rendendo così fattivo l'intento di comunicarlo ad altri - non si esaurirebbe automaticamente con la ricezione del messaggio e la presa di cognizione del suo contenuto da parte del destinatario, ma permarrebbe finché la comunicazione conservi carattere di attualità e interesse per i corrispondenti, venendo meno solo quando il decorso del tempo o altra causa abbia trasformato il messaggio in un documento "storico", cui attribuire un valore retrospettivo, affettivo, collezionistico, artistico, scientifico o probatorio. Così facendo, la Corte smentisce il pur consolidato orientamento della Corte di cassazione, che aveva statuito che i messaggi di posta elettronica, *SMS* e *WhatsApp*, già ricevuti e memorizzati nel computer o nel telefono cellulare del mittente o del destinatario, sarebbero stati da considerare come semplici «documenti» ai sensi dell'art. 234 c.p.p.[31].

Nella motivazione della Corte, la prima ragione per la quale l'orientamento della giurisprudenza di legittimità non può essere condiviso è, infatti, di ordine logico[32]. Se la ratio della disposizione costituzionale non è quella di prefigurare un privilegio del singolo parlamentare in quanto tale[33], ma una prerogativa «strumentale [...] alla salvaguardia delle funzioni parlamentari, volendosi impedire che intercettazioni e sequestri di corrispondenza possano essere indebitamente finalizzat[i] ad incidere sullo svolgimento del mandato elettivo, divenendo fonte di condizionamenti e pressioni sulla libera esplicazione dell'attività»[34], limitarla alle sole comunicazioni in corso di svolgimento e non

[31] In questo senso, tra le ultime, Cass. pen., sez. II, 19 ottobre 2022, n. 39529; Cass. pen., sez. VI, 8 giugno 2022, n. 22417; Cass. pen., sez. V, 6 maggio 2021, n. 17552, che hanno ritenuto quindi inapplicabile sia l'art. 254 c.p.p in materia di sequestro di corrispondenza, che l'art. 266 c.p.p. in materia di intercettazione nelle ipotesi di acquisizione di messaggi di natura elettronica recapitati (retro par. n. 2).

[32] Cfr. sul punto S. Curreri, *La libertà di comunicazione del parlamentare. Riflessioni sul "caso Renzi"*, in *LaCostituzione.info*, 2 marzo 2022, 2 ss; sia consentito un rinvio anche a P. Villaschi, *La posta elettronica e i messaggi WhatsApp sono corrispondenza?*, cit., 248-249.

[33] La libertà e segretezza delle cui comunicazioni è già protetta, infatti, dall'art. 15 Cost.

[34] Così Corte cost., 23 novembre 2007, n. 390; in senso analogo, Corte cost., 6 marzo 2019, n. 38, Corte

già concluse significherebbe, secondo la Corte, darne una interpretazione così restrittiva da limitare significativamente la suddetta tutela costituzionale ai casi, ormai rari, di corrispondenza cartacea e addirittura annullarla per i servizi di messaggistica istantanea e le *mail*, in cui all'invio segue immediatamente la ricezione[35]. Osserva in proposito, correttamente, il giudice costituzionale che «condizionamenti e pressioni sulla libera esplicazione del mandato parlamentare possono bene derivare, infatti, anche dalla presa di conoscenza dei contenuti di messaggi già pervenuti al destinatario»[36]. Peraltro, l'interpretazione proposta dalla giurisprudenza di legittimità e ripresa dalla Procura esporrebbe al rischio di un'elusione del dettato costituzionale da parte degli organi inquirenti, i quali anziché captare le comunicazioni nel momento in cui si svolgono, ne attenderebbero la conclusione (che nel caso dei messaggi elettronici è, come detto, pressoché coeva), per poi acquisire il dispositivo in cui vi è traccia del contenuto.

A ciò si aggiunga un profilo, su cui la Corte non era chiamata a pronunciarsi in quanto non oggetto del conflitto, ma che merita comunque una riflessione. Una lettura eccessivamente restrittiva della nozione di corrispondenza avrebbe minacciato la riservatezza delle comunicazioni anche della generalità dei cittadini, una volta che queste fossero state recapitate, consentendo «all'autorità di pubblica sicurezza di poter facilmente eludere tale tutela, sequestrando i messaggi via *mail*, *sms* o *WhatsApp* in casi asseritamente eccezionali di necessità ed urgenza che invece l'art. 15 Cost., a differenza dei precedenti due articoli sulla libertà personale e di domicilio, non prevede per la libertà di comunicazione»[37].

A sostegno della tesi qui prospettata la Corte adduce una serie di ulteriori argomenti. Anzitutto, rileva che, se la tutela di cui all'art. 15 Cost. e all'art. 68, c. 3, Cost. si estende anche ai dati esteriori delle comunicazioni in quanto essi stessi "fatti comunicativi"[38], non si vede come possano essere esclusi i messaggi *WhatsApp* e la posta elettronica dalla medesima copertura costituzionale. Nessuna differenza ontologica sussiste, infatti, tra una conversazione o una comunicazione e il documento che ne rivela i dati estrinseci quale il tabulato telefonico[39]. Anzi, come si era avuto già modo di osservare[40], il sequestro dei messaggi di posta elettronica e *WhatsApp* ha una capacità intrusiva

cost., 17 aprile 2013, n. 113.

35 Riprendendo quanto osservato da S. Curreri, *La libertà di comunicazione*, cit., 1. Sul punto, v. anche G. Guzzetta, *La nozione di comunicazione*, cit., 84, che evidenzia come la Corte ricorra qui ad una *reductiu ad absurdum*.

36 Corte cost., 27 luglio 2023, n. 170, Considerato in Diritto n. 4.4.

37 Sempre S. Curreri, *La libertà di comunicazione*, cit., 2.

38 Il riferimento è, chiaramente, ai tabulati telefonici, documenti che consentono di aprire squarci di conoscenza sui rapporti di un parlamentare «di ampiezza ben maggiore rispetto alle esigenze di una specifica indagine e riguardanti altri soggetti (in specie, altri parlamentari) per i quali opera e deve operare la medesima tutela dell'indipendenza e della libertà della funzione», in questi termini, Corte cost., 6 marzo 2019, n. 38, Considerato in Diritto n. 2.4. A commento, cfr. F. Girelli, *La "legittimità" della tutela dello spazio comunicativo del parlamentare*, in *Osservatorio AIC*, 1, 2020, 240 ss.; R. Orlandi, *Tabulati telefonici e immunità parlamentare*, in *Giurisprudenza costituzionale*, 2, 2019, 678 ss; M. Violante, *Tabulati telefonici relativi a parlamentari tra autorizzazione e dubbi di legittimità costituzionale*, in *Processo penale e giustizia*, 5, 2019, 1101 ss.

39 Così Corte cost., 27 luglio 2023, n. 170, Considerato in Diritto n. 4.3.

40 Sul punto sia consentito rinviare a P. Villaschi, *La posta elettronica e i messaggi WhatsApp sono corrispondenza?*, cit., 250-251.

addirittura maggiore a quella dell'acquisizione dei tabulati, dal momento che non solo è possibile risalire ai dati identificativi estrinseci delle comunicazioni, ma anche al contenuto.

Inoltre, il Giudice delle Leggi richiama nuovamente la citata giurisprudenza della Corte Europea dei Diritti dell'Uomo, che, non solo, come osservato retro al par. n. 2.1., aveva ricondotto sotto la nozione di corrispondenza le comunicazioni elettroniche, ma specificamente anche i messaggi già recapitati e conservati sul dispositivo del destinatario. Due le pronunce più significative al riguardo. La prima è quella relativa al caso Bărbulescu c. Romania, con la quale la Corte di Strasburgo, per la prima volta, incluse nel concetto di corrispondenza un servizio di messaggistica istantanea quale Yahoo Messenger. Si trattava di un software, sviluppato da Yahoo! a partire dal 1998 e in funzione sino al 2018, che consentiva lo scambio in tempo reale di brevi messaggi tra gli utenti, così configurandosi come uno dei precursori proprio di *WhatsApp*. Nell'accogliere il ricorso di un cittadino rumeno, che lamentava di essere stato licenziato dopo che il proprio datore di lavoro, accedendo alle comunicazioni private del ricorrente, aveva verificato che quest'ultimo aveva fatto ricorso al servizio di messaggistica dall'account della società per finalità esclusivamente personali, i giudici di Strasburgo affermavano che «il tipo di servizio di messaggeria istantanea mediante internet in questione è soltanto una delle forme di comunicazione che permettono alle persone di condurre una vita sociale privata. Allo stesso tempo, l'invio e la ricezione di comunicazioni sono compresi nella nozione di "corrispondenza"»[41]. La seconda decisione è la sentenza Saber c. Norvegia[42], con la quale la Corte EDU confermava che la tutela di cui all'art. 8 CEDU si estende alla corrispondenza "conservata" sul dispositivo del destinatario (in quel caso un telefono cellulare posto sotto sequestro).

Infine, la Corte costituzionale, a sostegno del fatto che i messaggi *WhatsApp* e di posta elettronica recapitati sono da considerarsi a tutti gli effetti corrispondenza, richiama quel filone della giurisprudenza di legittimità che aveva delineato i confini dei già richiamati artt. 616 e 617 c.p., rubricati rispettivamente "Violazione, sottrazione e soppressione di corrispondenza" e "Cognizione, interruzione o impedimento di illeciti di comunicazioni o conversazioni telegrafiche o telefoniche". Ad avviso di tale giurisprudenza «pur nell'ambito di una non nitida sistematica quale è quella che caratterizza le incriminazioni poste a tutela della inviolabilità delle comunicazioni, deve ritenersi che la possibile interferenza tra le fattispecie punite dagli artt. 616 e 617 c.p. (determinata dalla comune previsione della condotta di colui che prende cognizione della corrispondenza o delle comunicazioni altrui) sia solo apparente»[43]. Le stesse hanno, infatti, ambiti operativi ben definiti dalla diversa configurazione dell'oggetto materiale della condotta, anche indipendentemente dalle specifiche connotazioni modali che la caratterizzano nell'art. 617 c.p. e che, invece, non sono previste nell'art. 616 c.p. Pertanto, l'art. 617 c.p. si riferirebbe al profilo "dinamico" della comunicazione umana, come suggerirebbero anche l'ulteriore termine dispiegato per definire l'oggetto materiale del reato ("conversazione") e le condotte alternative a quella di fraudolenta

41 CEDU, *Bărbulescu c. Romania*, cit., §§ 72 e 74.

42 CEDU, *Saber c. Norvegia,* cit., §§ 48-51.

43 Cass. pen., sez. V, 4 novembre 2020, n. 30735.

cognizione idonee ad integrare il fatto tipico (interrompere ed impedire). Nell'art. 616 c.p. il concetto di "corrispondenza" risulterebbe invece funzionale ad individuare la comunicazione umana nel suo profilo "statico" e cioè «il pensiero già comunicato o da comunicare fissato su supporto fisico o altrimenti rappresentato in forma materiale»[44]. Tanto è vero che la Suprema Corte concludeva rilevando come la condotta contestata all'imputato in quel caso - e cioè aver preso cognizione del contenuto della corrispondenza telematica intercorsa tra due soggetti estranei conservata nell'archivio di posta elettronica di uno di loro - proprio in virtù della configurazione del suo oggetto materiale, doveva essere ricondotta nell'alveo dell'art. 616 c.p. e non già, come ritenuto dai giudici di merito, in quello dell'art. 617, c. 1, c.p. Sulla base di tali premesse, il giudice di legittimità era giunto alla conclusione che i messaggi di natura telematica conservati nel dispositivo del destinatario fossero da considerarsi allora come "corrispondenza" (nella sua accezione più propriamente "statica")[45].
Al medesimo esito perviene la Corte costituzionale, chiarendo, in definitiva, che le guarentigie dell'art. 15 Cost. per la generalità dei cittadini e quelle aggiuntive dell'art. 68, c. 3, Cost. per i soli parlamentari si estendono anche ai messaggi recapitati e conservati sul dispositivo del destinatario.

2.3. La precisazione relativa alla natura del conto corrente bancario

Ad un esito differente il giudice costituzionale giunge con riferimento all'acquisizione del conto corrente bancario del senatore Renzi da parte degli inquirenti (n. 4.5 del Considerato in Diritto).
Nel sostenere che, anche in questo caso, si configurasse un sequestro di corrispondenza, il Senato aveva fatto leva in particolare sulla circostanza che l'estratto del conto corrente - ossia il prospetto redatto dalla banca, nel quale sono riportati tutti i movimenti di dare e di avere verificatisi nel conto durante un dato lasso temporale - deve formare oggetto di periodica spedizione al correntista[46]. L'art. 119 del T.U. bancario prevede infatti, in via generale, al c. 1, che nei contratti di durata la banca fornisce al cliente, alla

[44] Cfr., sempre, Cass. pen., sez. V, 4 novembre 2020, n. 30735, che riprende Cass. pen., sez. V, 2 maggio 2019, n. 18284; Cass., sez. II, 28 novembre 2017, n. 952; Cass. pen., sez. II, 15 marzo 2017, n. 12603.

[45] In materia civile, rileva, invece, Cass., sez. Lavoro, ord. 10 settembre 2018, n. 21965, ove si evidenziava che «l'esigenza di tutela della segretezza nelle comunicazioni si impone anche a riguardo ai messaggi di posta elettronica scambiati tramite mailing list riservata agli aderenti ad un determinato gruppo di persone, alle newsgroup o alle chat private, con accesso condizionato al possesso di una password fornita a soggetti determinati». Tanto è vero che, scrivevano gli ermellini, «i messaggi che circolano attraverso le nuove forme di comunicazione, ove inoltrati non ad una moltitudine indistinta di persone, ma unicamente agli iscritti a un determinato gruppo, come nelle chat private o chiuse, devono essere considerati alla stregua della corrispondenza privata, chiusa e inviolabile».

[46] In dottrina si registra una tendenziale contrapposizione fra coloro che qualificano il conto corrente bancario come "contratto innominato misto", risultante dall'unione di più prestazioni tipiche di altri contratti nominati e coordinate intorno ad una prestazione principale di mandato (A. Fiorentino, *Del conto corrente. Dei contratti bancari*, in *Comm. Scialoja, Branca, sub artt. 1823-1860*, Bologna-Roma, 1972, 164) e quanti ne affermano la tipicità (N. Salanitro, *Conto corrente bancario*, in *Digesto comm.*, IV, Torino, 1989, 10).

scadenza del contratto e, comunque sia, almeno una volta l'anno, «una comunicazione chiara in merito allo svolgimento del rapporto» e precisa, al c. 2, che per i «rapporti regolati in conto corrente» l'estratto conto è inviato con periodicità annuale o con quella più breve - semestrale, trimestrale o mensile - prescelta dal cliente. Per tali ragioni, ad avviso del Senato, l'estratto conto si sarebbe configurato come una comunicazione, riservata, della banca nei confronti del cliente, potendosi annoverare nel più ampio concetto di "corrispondenza bancaria", con conseguente applicazione delle garanzie di cui all'art. 15 Cost. (e per i parlamentari di quelle aggiuntive di cui all'art. 68, c. 3, Cost.). In questo senso avrebbe deposto sia l'orientamento di parte della dottrina[47] sia alcune pronunce della Cassazione[48].

La Corte costituzionale non smentisce tale ricostruzione, tanto da sottolineare che se oggetto di apprensione da parte degli organi inquirenti fosse effettivamente stato l'estratto conto spedito dalla banca al correntista (ossia al senatore Renzi) avrebbero operato le guarentigie costituzionali di cui si discorre. Ciò, tuttavia, non si era verificato nello specifico caso di specie, dal momento che l'estratto conto del senatore era entrato negli atti di indagine in altro modo, ossia tramite un decreto di acquisizione di segnalazioni di operazioni bancarie sospette effettuate in base alla normativa antiriciclaggio di cui al d.lgs. 231/2007, tra le quali figurava appunto il documento in questione, ricavato dalla segnalante Unità di informazione finanziaria della Banca d'Italia tramite interrogazione delle banche dati in suo possesso. In una simile, peculiare, ipotesi non ci si trova allora di fronte, ad avviso della Corte, ad un sequestro di corrispondenza, poiché manca, all'origine, un'attività di comunicazione e di spedizione. Il conto corrente di per sé, infatti, è un documento contabile interno della banca e il fatto che debba, in taluni casi, essere trasmesso al cliente non lo qualifica in automatico come corrispondenza, quantomeno fintanto che tale invio non si verifichi. Né ad una conclusione differente può giungersi in ragione del fatto che esso contiene dati riservati del cliente. Ricorda, infatti, la Corte che l'art. 68, c. 3, Cost. non tutela genericamente la riservatezza del parlamentare, che sotto questo punto di vista gode delle medesime garanzie previste dall'ordinamento per la generalità dei cittadini[49]. Tanto premesso, il ricorso del Senato, limitatamente a tale atto investigativo, non può quindi essere accolto.

Trattasi di un passaggio della motivazione, a prima vista di minore rilevanza, ma in realtà interessante, offrendo al Giudice delle Leggi l'occasione per chiarire la portata applicativa e la ratio di fondo delle disposizioni costituzionali di cui si tratta. Quanto all'art. 68 Cost., non va, infatti, dimenticato che la disposizione costituzionale richiede l'autorizzazione della Camera di appartenenza esclusivamente per eseguire specifici e tassativi atti nei confronti dei membri del Parlamento particolarmente suscettibili di incidere sullo svolgimento del mandato elettivo[50], non rispondendo la disposizione

[47] In particolare, si v. l'analisi di M. Cerase, *Art. 68*, in R. Bifulco-A. Celotto-M. Olivetti (a cura di), *Commentario alla costituzione*, Torino, 2006, 1304 ss.

[48] È stata, infatti, ritenuta integrare la fattispecie del più volte menzionato art. 616 c.p. l'apertura da parte del marito della corrispondenza chiusa, destinata alla moglie, contenente l'estratto conto inviato a quest'ultima dalla banca (Cass. pen., sez. II, 12 gennaio 2018, n. 952, in *Dir. Pen. e Processo*, 3, 2018, 343).

[49] Corte cost., 27 luglio 2023, n. 170, Considerato in Diritto n. 4.5.

[50] E nello specifico al c. 2: limitazioni della libertà personale, perquisizioni personali e domiciliari; al c. 3: intercettazioni e sequestri di corrispondenza, cfr., *ex plurimis*, v. M. Cerase, *Anatomia critica delle immunità*

costituzionale ad altre esigenze. Quanto, invece, al perimetro applicativo del concetto di corrispondenza, la precisazione della Corte è importante, poiché sottolinea come sia pregiudiziale la sussistenza di una "trasmissione", nel senso di uno scambio di pensiero tra due o più soggetti determinati, senza la quale risulta inutile ogni altro ragionamento sugli ulteriori requisiti di cui si è detto retro al par. n. 2.

3. L'interpretazione offerta in merito allo schema procedurale applicabile ai sensi della l. 140/2003 nelle ipotesi di sequestro di corrispondenza

Chiarito come le comunicazioni di natura elettronica siano, a tutti gli effetti, corrispondenza, la Corte, al punto n. 5.1 del Considerato in Diritto, passa all'individuazione del modulo procedurale applicabile ai sensi della l. 140/2003 alle ipotesi di sequestro di corrispondenza in cui siano coinvolti parlamentari.

Sul punto, come noto, la giurisprudenza costituzionale in materia di intercettazioni di conversazioni e comunicazioni ed acquisizione di tabulati telefonici, a partire dalla sentenza n. 390 del 2007, ha sempre distinto tra intercettazioni "mirate" (dirette o indirette), da una parte, rispetto alle quali è necessaria l'autorizzazione preventiva della Camera di appartenenza *ex* art. 4 della legge menzionata, e quelle "casuali", dall'altra, per le quali si richiede esclusivamente l'autorizzazione successiva all'utilizzo del materiale investigativo nei confronti del parlamentare (mentre nessuna autorizzazione è necessaria per l'utilizzo nei confronti di terzi), *ex* art. 6 della legge in questione[51].

In particolare, la disciplina dell'autorizzazione preventiva, delineata dall'art. 4 cit. in attuazione dell'art. 68 Cost., il quale «vieta di sottoporre ad intercettazione, senza autorizzazione, non le utenze del parlamentare, ma le sue comunicazioni», deve trovare applicazione «tutte le volte in cui il parlamentare sia individuato in anticipo quale destinatario dell'attività di captazione»: dunque, non soltanto quando siano sottoposti ad intercettazione utenze o luoghi appartenenti al soggetto politico o nella sua disponibilità (c.d. intercettazioni "dirette"), ma anche tutte le volte in cui la captazione si riferisca ad utenze di interlocutori abituali del parlamentare o sia effettuata in luoghi presumibilmente da questo frequentati, al precipuo scopo di conoscere il contenuto delle conversazioni e delle comunicazioni del parlamentare stesso (c.d. intercettazioni indirette-mirate). E ciò che rileva al fine di distinguere tali intercettazioni da quelle casuali non è la titolarità o la disponibilità dell'utenza captata, ma la direzione dell'atto di indagine, dal momento che «se quest'ultimo è volto, in concreto, ad accedere nella sfera delle comunicazioni del parlamentare, l'intercettazione non autorizzata è illegittima, a prescindere dal fatto che il procedimento riguardi terzi o che le utenze sottoposte a controllo appartengano a terzi». Viceversa, la disciplina dell'autorizzazione successiva,

parlamentari italiane, Rubbettino, 2011, 101 ss.

[51] Su tale distinzione si rinvia alle autorevoli riflessioni, elaborate all'indomani della sentenza Corte cost., 23 novembre 2007, n. 390, da N. Zanon, *Il regime delle intercettazioni "indirette" e "occasionali" fra principio di parità di trattamento davanti alla giurisdizione e tutela della funzione parlamentare*, in *Federalismi*, 23, 2007, 1 ss.; T. F. Giupponi, *Le intercettazioni «indirette» nei confronti dei parlamentari: cronaca di un'illegittimità costituzionale (pre)annunciata*, in *Quaderni costituzionali*, 1, 2008, 150 ss.

prevista dall'art. 6 cit., si riferisce unicamente alle intercettazioni "casuali", rispetto alle quali «proprio per il carattere imprevisto dell'interlocuzione del parlamentare, l'autorità giudiziaria non potrebbe, neanche volendo, munirsi preventivamente del *placet* della Camera di appartenenza»[52].

Orbene, muovendo dall'assunto che i principi affermati dalla giurisprudenza costituzionale con riferimento alle intercettazioni e ai tabulati telefonici fossero *tout court* applicabili anche alle ipotesi di sequestro di corrispondenza, il ricorso del Senato era fondamentalmente teso a dimostrare il carattere "non casuale" dell'attività investigativa disposta dalla Procura di Firenze. Ciò al precipuo fine di sottolineare la necessità di un'autorizzazione preventiva *ex* art. 4 della l. 140/2003, autorizzazione mai richiesta da parte dell'autorità giudiziaria e, in questo modo, sostenere l'illegittimità dei sequestri disposti. Tanto è vero che, sempre nel ricorso in commento, si rilevava che dai decreti di perquisizione e sequestro emessi a carico di Ugo Manes e Marco Carrai, presso i quali era stata sequestrata, acquisita e trasfusa negli atti di indagine la corrispondenza con il senatore Renzi, sarebbe stato chiaramente desumibile che la direzione dell'atto di indagine fosse diretta ad accedere nella sfera delle comunicazioni e conversazioni del parlamentare[53]. Di avviso contrario la Procura, che aveva rilevato di non aver svolto alcuna attività investigativa nei confronti del parlamentare, né di avere elementi per ritenere che i dott. Manes e Carrai intrattenessero rapporti di corrispondenza con l'onorevole Renzi, così escludendo qualsiasi intento persecutorio nei confronti del senatore e, pertanto, la necessità di richiedere un'autorizzazione preventiva al Senato.

Nessuno delle due parti si era però preoccupata di riflettere attorno ad un profilo, evidenziato in dottrina[54] ed emerso anche nella riunione della Giunta delle elezioni e delle immunità parlamentari del Senato del 14 dicembre 2021[55], ossia che la l. 140/2003 presenta due formulazioni differenti, a seconda che si prenda in considerazione l'art. 4 o l'art. 6 cit.; nel primo caso, infatti, la disposizione, nel disciplinare l'autorizzazione ex ante, così recita: «quando occorre eseguire nei confronti di un membro del Parlamento perquisizioni personali o domiciliari, ispezioni personali, intercettazioni, in qualsiasi forma, di conversazioni o comunicazioni, sequestri di corrispondenza, o acquisire tabulati di comunicazioni, ovvero, quando occorre procedere al fermo, all'esecuzione di una misura cautelare personale coercitiva o interdittiva ovvero all'esecuzione dell'accompagnamento coattivo, nonché di misure di sicurezza o di prevenzione aventi natura personale e di ogni altro provvedimento privativo della libertà personale, l'autorità competente richiede direttamente l'autorizzazione della Camera alla quale il soggetto appartiene […]». Al contrario, l'art. 6, nel regolare l'autorizzazione ex post all'utilizzo, ha una portata più ristretta, statuendo che: «1. Fuori dalle ipotesi previste

[52] Corte cost., 23 novembre 2007, n. 390, Considerato in Diritto n. 5.3. Tale distinzione tra intercettazioni mirate e casuali è stata confermata nelle successive pronunce che hanno avuto ad oggetto l'applicazione dell'art. 68, c. 3, Cost., ad esempio sentenze Corte cost., 25 marzo 2010, n. 114, Corte cost., 25 marzo 2010, n. 113 e, più di recente, Corte cost., 6 marzo 2019, n. 38.

[53] Cfr. ricorso per conflitto di attribuzione tra poteri dello Stato n. 10 del 2022, promosso dal Senato della Repubblica, cit., 14-15.

[54] Cfr. ad esempio E. Albanesi, *Messaggistica WhatsApp*, cit., spec. 99-108.

[55] Cfr. Relazione della Giunta delle elezioni e delle immunità parlamentari del 14 dicembre 2021, cit., 3-5.

dall'articolo 4, il giudice per le indagini preliminari, anche su istanza delle parti ovvero del parlamentare interessato, qualora ritenga irrilevanti, in tutto o in parte, ai fini del procedimento i verbali e le registrazioni delle conversazioni o comunicazioni intercettate in qualsiasi forma nel corso di procedimenti riguardanti terzi, alle quali hanno preso parte membri del Parlamento, ovvero i tabulati di comunicazioni acquisiti nel corso dei medesimi procedimenti, sentite le parti, a tutela della riservatezza, ne decide, in camera di consiglio, la distruzione integrale ovvero delle parti ritenute irrilevanti, a norma dell'articolo 269, commi 2 e 3, del codice di procedura penale». Dal che si ricava che all'art. 6 citato manca un riferimento al sequestro di corrispondenza, regolando la disposizione in esame esclusivamente le ipotesi di autorizzazione ex post all'utilizzo dei verbali delle intercettazioni o dei tabulati telefonici.

Proprio sulla base di questa differente formulazione, la Giunta aveva concluso che nelle ipotesi di sequestro di corrispondenza l'unica disposizione applicabile fosse l'art. 4 della l. 140/2003 e, quindi, lo schema procedurale quello dell'autorizzazione preventiva, precisando che, qualora ad essere posto sotto sequestro fosse il dispositivo di un terzo e l'autorità inquirente vi rinvenisse corrispondenza con un parlamentare, essa avrebbe dovuto immediatamente inviare la richiesta di autorizzazione alla Camera di appartenenza e astenersi, nel mentre, da ogni attività[56].

Ed è proprio quest'ultima la prospettiva accolta dalla Corte costituzionale nella decisione in esame, nonostante, come detto, nessuna delle due parti (né il Senato né la Procura) l'avesse fatta propria.

Nello specifico, il giudice costituzionale muove dalla preliminare considerazione che i dispositivi sequestrati dagli inquirenti, che non appartenevano direttamente al senatore Renzi ma a terzi (i dott. Carrai e Manes), vadano considerati come «contenitori di dati informatici appartenenti a terzi – telefoni cellulari, ma potrebbe trattarsi, allo stesso modo, di computer o di altri dispositivi – nella cui memoria erano conservati, tra l'altro,

[56] Cfr. Relazione della Giunta delle elezioni e delle immunità parlamentari del 14 dicembre 2021, cit., 4, ove si legge «per il "sequestro di corrispondenza", il modulo procedurale applicabile è solo quello dell'art. 4 della legge n. 140 del 2003, ossia quello dell'autorizzazione *ex ante*. Ovviamente, quando viene reperita corrispondenza elettronica sul cellulare sequestrato ad un terzo non parlamentare, l'autorità giudiziaria, ove si accorga della presenza di corrispondenza elettronica intercorsa con un senatore, deve immediatamente inviare richiesta al Senato». A suffragare tale tesi la Giunta richiamava in particolare un precedente, che aveva avuto ad oggetto la richiesta della Procura della Repubblica presso il Tribunale di Milano di autorizzazione ad eseguire un sequestro di corrispondenza nei confronti del senatore Armando Siri, corrispondenza contenuta nello smartphone di proprietà ed in uso al collaboratore Marco Luca Perini; la richiesta era stata giustificata dall'esigenza di acquisire conversazioni telefoniche, messaggistiche, mail e chat presenti nel telefono del collaboratore e intercorse con il senatore stesso, nell'ambito di un procedimento penale pendente nei confronti di entrambi (in quel caso si trattava, in particolare, di un'ipotesi di concorso nel reato di auto-riciclaggio aggravato). Ebbene, in quell'occasione, lo stesso Pubblico ministero, nel fare riferimento al terzo comma dell'art. 68 della Costituzione precisava di aver sospeso l'esecuzione del provvedimento ai sensi dell'art. 4, c. 2, della legge n. 140 del 2003 ed, illustrate le esigenze investigative poste a base della domanda, chiedeva al Senato della Repubblica l'autorizzazione ex ante ad eseguire il sequestro di corrispondenza del senatore Armando Siri contenuta nello smartphone di proprietà ed in uso al collaboratore. Tuttavia, giova precisare che quel precedente non pare particolarmente conferente dal momento che, in quel caso, la lettura del resoconto della stessa Giunta suggerisce come l'attività investigativa fosse stata ab origine mirata. Per maggiori dettagli si veda la Relazione della Giunta delle elezioni e delle immunità parlamentari del Senato della Repubblica sulla domanda di autorizzazione a eseguire un sequestro di corrispondenza nei confronti del senatore Armando Siri con riferimento al suo collaboratore Marco Luca Perini, 13 novembre 2019, doc. IV n. 4-a, 1-5.

messaggi inviati in via telematica a un parlamentare, o da lui provenienti». In altre parole, la Corte distingue tra contenitore (il dispositivo) e il contenuto (la corrispondenza telematica). In una simile evenienza, gli organi inquirenti possono disporre il sequestro del "contenitore" (nella specie, del dispositivo di telefonia mobile). Nel momento, però, in cui riscontrano la presenza in esso di messaggi intercorsi con un parlamentare, devono sospendere l'estrazione di tali messaggi dalla memoria del dispositivo (o dalla relativa copia) e chiedere l'autorizzazione, preventiva, alla Camera di appartenenza del parlamentare, a norma dell'art. 4 della l. 140/2003, al fine di poterli coinvolgere nel sequestro. Proprio come sostenuto dalla Giunta, ad avviso della Corte, «l'autorizzazione va chiesta, nei termini dianzi delineati, a prescindere da ogni valutazione circa la natura "mirata" o "occasionale" dell'acquisizione dei messaggi del parlamentare, operata tramite l'apprensione dei dispositivi appartenenti a terzi». Ciò in quanto la distinzione tra captazione indirette-mirate e casuali elaborata con riferimento alle intercettazioni di conversazioni o comunicazioni non è riferibile alla fattispecie del sequestro di corrispondenza. Il motivo risiede nella circostanza che «diversamente che nel caso delle intercettazioni - le quali consistono in una attività prolungata nel tempo di captazione occulta di comunicazioni o conversazioni che debbono ancora svolgersi nel momento in cui l'atto investigativo è disposto - qui si discute dell'acquisizione uno actu di messaggi comunicativi già avvenuti. Una volta riscontrato che si tratta di messaggi di un parlamentare, o a lui diretti, diviene, quindi, in ogni caso operante la guarentigia di cui all'art. 68, terzo comma, Cost.»[57].

In definitiva, ad avviso della Corte, «il modulo procedurale che si è delineato garantisce, d'altro canto, un punto di equilibrio tra gli interessi in gioco […]. Quando pure, infatti, gli organi inquirenti possano prevedere che nel telefono cellulare o nel computer di una persona sottoposta ad indagini siano memorizzati messaggi di un parlamentare, ciò non impedisce, comunque sia, agli organi stessi di apprendere il dispositivo e di sequestrare tutti gli altri dati informatici contenuti nel dispositivo, che nulla hanno a che vedere con la corrispondenza del parlamentare: fermo restando invece l'onere della richiesta di autorizzazione al fine di estrapolare dal dispositivo e di acquisire agli atti del procedimento i messaggi che riguardano il parlamentare stesso». La ricostruzione prospettata spiegherebbe, d'altro canto, nella prospettiva del giudice costituzionale, perché il citato art. 6 cit. non abbia esteso la disciplina dell'autorizzazione successiva al sequestro di corrispondenza, dal momento che in questo caso la natura occasionale o mirata dell'atto non verrebbe proprio in considerazione, risultando in ogni caso necessaria l'autorizzazione preventiva[58].

La soluzione offerta dalla Corte è certamente interessante e ha il pregio di offrire una

[57] L'estrazione dei dati non è, infatti, ad avviso della Corte, un «*posterius* rispetto all'esecuzione dell'atto investigativo per il quale è prefigurata la garanzia in questione. In senso contrario, va osservato che nel caso di sequestro probatorio informatico il "vero" oggetto del sequestro non è tanto il dispositivo elettronico (il "contenitore") – il quale, di per sé, non ha di norma alcun interesse per le indagini – quanto piuttosto i suoi dati (il "contenuto"), nella parte in cui risultano utili alle indagini stesse: dati che, secondo le indicazioni della giurisprudenza di legittimità, vanno all'uopo selezionati e fatti possibilmente oggetto di una "copia-clone", con restituzione del dispositivo (e della disponibilità di tutti gli altri dati) al titolare».

[58] Tutti i passaggi riportati sono tratti da Corte cost., 27 luglio 2023, n. 170, Considerato in Diritto n. 5.1.

risposta chiara ad una questione interpretativa piuttosto intricata e controversa. Lo "schema procedurale" proposto può, quindi, essere riassunto come segue: a) nessuna preclusione discende dall'art. 68, c. 3, Cost. per disporre il sequestro del dispositivo di proprietà di un terzo; b) qualora ciò avvenga, nessuna verifica in merito alla direzione dell'atto di indagine è necessaria da parte dell'autorità inquirente; c) tuttavia, nel caso siano rinvenute all'interno del dispositivo sequestrato conversazioni con un parlamentare, il pubblico ministero è tenuto a richiedere, immediatamente, l'autorizzazione preventiva *ex* art. 4 della l. 140/2003 alla Camera di appartenenza, altrimenti l'estrazione della corrispondenza tra terzo e parlamentare è illegittima.

Nonostante la chiarezza e praticità del modulo procedurale qui delineato, alcuni passaggi della motivazione scontano alcuni margini di ambiguità su cui può essere di interesse sollecitare una riflessione aggiuntiva.

Da questo punto di vista, in altra sede[59], si era provato a offrire una possibile soluzione alternativa al quesito in esame, muovendo dal presupposto che il consolidato orientamento che distingueva tra attività investigativa diretta/mirata, da una parte, e casuale, dall'altra, dovesse tenersi fermo anche con riferimento ai sequestri di corrispondenza e fosse, quindi, necessario procedere ad una valutazione della direzione dell'atto di indagine. In particolare, la casualità del sequestro si sarebbe avuta tutte le volte in cui il pubblico ministero fosse riuscito a dimostrare di non essersi prefigurato la possibilità che tra i messaggi conservati all'interno del dispositivo del terzo ve ne fossero alcuni diretti ad un membro del Parlamento[60].

Tale soluzione non è stata, tuttavia, accolta dalla Corte, che, come visto, giustifica la scelta distinguendo, anzitutto, tra contenitore (il dispositivo) e contenuto (la corrispondenza) e rilevando che, nelle ipotesi del sequestro di corrispondenza, si è in presenza di un'acquisizione *uno actu* di messaggi comunicativi già avvenuti.

Sul punto possono, in particolare, svolgersi le seguenti considerazioni.

Anzitutto, per quanto sicuramente la distinzione contenitore/contenuto sia convincente, è lo stesso giudice costituzionale a rilevare che nel sequestro informatico il "vero" oggetto del sequestro non è tanto il dispositivo elettronico (il contenitore) quanto piuttosto i suoi dati (il contenuto). Cosa che allora avrebbe potuto suggerire la necessità di una valutazione complessiva dell'attività investigativa, il cui scopo non è tanto il sequestro del contenitore (il telefono, per fare un esempio), ma appunto del contenuto (la corrispondenza telematica).

In secondo luogo, non persuade del tutto la scelta di escludere, alla radice, la possibilità anche solo di valutare la sussistenza della casualità con riferimento ai sequestri di corrispondenza in ragione del fatto che la comunicazione è, in questi casi, già avvenuta. In disparte il fatto che possono ben verificarsi anche sequestri di corrispondenza *in itinere* (è il caso dell'art. 254 c.p.p., come ricorda la stessa Corte), la circostanza che solitamente, quando si tratta di corrispondenza, la comunicazione sia già conclusa potrebbe non

[59] Sia consentito un rinvio a quanto rilevato, a commento del ricorso, in P. Villaschi, *La posta elettronica e i messaggi WhatsApp sono corrispondenza?*, cit., spec. 257-263.

[60] Sulla specifica questione delle acquisizioni probatorie informatiche cfr. le indizioni di Cass. pen., sez. VI, 22 settembre 2020, n. 34265, in *Foro It.*, 2021, 2, 6, 402, con nota di M. Pittiruti, *Dalla corte di cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus*, in *Sistema Penale*, 1, 2021.

essere dirimente. Sul punto si sarebbe potuto richiamare un significativo precedente, ossia la sentenza n. 38 del 2019 in materia di tabulati telefonici. In quell'occasione il Giudice delle Leggi dichiarò non fondata la questione di legittimità sollevata con riferimento all'art. 6, c. 2, della l. 140/2003, nella parte in cui prevedeva che il giudice debba chiedere alla Camera di appartenenza l'autorizzazione successiva ad utilizzare i tabulati di comunicazioni relativi ad utenze intestate a terzi venute in contatto con un parlamentare. Tabulati che la Corte qualificava come "dati puramente storici ed esteriori", in altre parole "fatti comunicativi", avvenuti e conclusi. Ebbene, nel rigettare la questione sull'art. 6 cit., il giudice costituzionale implicitamente riconobbe la possibilità che potesse verificarsi l'acquisizione casuale di un tabulato telefonico, e, quindi, di un "fatto comunicativo concluso"[61]. Lo stesso ragionamento si sarebbe forse potuto estendere alla corrispondenza.

È pur vero che, come evidenzia la Corte, il riferimento all'acquisizione dei tabulati telefonici compare non solo all'art. 4, ma anche all'art. 6 della l. 140/2003, a differenza del sequestro di corrispondenza, e questo potrebbe in effetti spingere nella direzione di escludere in radice possibili sequestri di corrispondenza casuali a carico dei parlamentari. La differente formulazione legislativa si sarebbe potuta leggere, tuttavia, in modo differente. L'assenza di un riferimento al sequestro di corrispondenza all'art. 6 cit. avrebbe potuto, infatti, portare alla diversa conclusione che nessuna autorizzazione (nemmeno successiva) sarebbe stata necessaria nel caso in cui fosse stata accertata la casualità dell'attività investigativa. In caso di sequestro, invece, diretto o comunque mirato sarebbe stata chiaramente necessaria l'autorizzazione preventiva ai sensi dell'art. 4 cit[62]. Una simile prospettiva sarebbe stata avvalorata dal fatto che, come affermato dalla Corte costituzionale sin dalla sentenza n. 390 del 2007, la previsione di cui all'art. 68, c. 3, Cost. risulta interamente soddisfatta, a livello di legge ordinaria, dall'art. 4 della l. 140/2003, mentre l'autorizzazione successiva prevista dall'art. 6 della l. 140/2003, la cui *ratio* è differente, non è costituzionalmente imposta[63]. In definitiva, si sarebbe forse potuto sostenere che il legislatore, nel formulare l'art. 6 cit., avesse, nella sua discrezionalità, scelto di introdurre una previsione, costituzionalmente non necessaria (a differenza dell'art. 4 cit., vera e propria norma di attuazione dell'art. 68 Cost.) per tutelare ulteriormente i parlamentari (e, in origine, prima dell'intervento della sentenza n. 390 del 2007, anche i terzi) dalle sole attività di intercettazione e di acquisizione dei tabulati, di natura casuale, senza estendere la previsione anche ad altri atti investigativi, pure contemplati nell'art. 4 cit.

---

[61] Nello stesso senso, può leggersi la sent. della Corte cost., 28 maggio 2010, n. 188, ove non si obiettò che l'acquisizione di tabulati di utenze di altri indagati fosse avvenuta al fine di eludere l'autorizzazione preventiva all'acquisizione dei tabulati delle utenze del parlamentare e, dunque, che, in altre parole, si applicasse il censurato art. 6, c. 2.

[62] A testimonianza della pluralità di interpretazioni prospettabili, a commento del ricorso sollevato dal Senato, in dottrina, muovendo dal presupposto che la distinzione tra attività investigativa diretta/mirata e casuale si dovesse applicare anche ai sequestri di corrispondenza, si era anzi avanzata l'ipotesi di un'auto-rimessione da parte della stessa Corte della questione di legittimità costituzionale dell'art. 6 della legge n. 140 del 2003, nella parte in cui non prevede, tra le fattispecie ivi presenti, anche quella del «sequestro della corrispondenza», in parallelismo con l'art. 4 della stessa legge, cfr. E. Albanesi, *Messaggistica WhatsApp,* cit., spec. 102-105.

[63] In questo senso cfr. N. Zanon, *Il regime delle intercettazioni,* cit., 3.

Se questa poteva essere una possibile strada alternativa, ad ogni modo, la Corte costituzionale sposa una differente soluzione, dichiarando conseguentemente che non spettava alla Procura acquisire agli atti la messaggistica *WhatsApp* e di posta elettronica tra il senatore Renzi e i dott. Carrai e Manes, rinvenuta sui dispositivi di questi ultimi in assenza dell'autorizzazione richiesta dall'art. 4 cit.
In definitiva, la soluzione individuata, da un lato, ha il pregio di offrire un chiarimento atteso in merito alla diversa formulazione degli artt. 4 e 6 della l. 140/2003, proporre uno schema procedurale di agevole applicazione e consentire alle autorità inquirenti di procedere all'estrazione di tutta la corrispondenza rinvenuta sul dispositivo di un terzo che non abbia come destinatario un membro del Parlamento; dall'altro, sconta alcune ambiguità relative alla linearità del percorso argomentativo seguito e potrebbe inoltre rivelarsi eccessivamente "garantista", dal momento che, così facendo, il mero rinvenimento di una corrispondenza con un parlamentare sul dispositivo di un privato cittadino impone di richiedere l'autorizzazione preventiva e, nel caso questa sia negata, comporta l'impossibilità di procedere all'estrazione e, quindi, all'acquisizione della corrispondenza in oggetto nei confronti di entrambi (non solo il parlamentare, quindi, ma anche il terzo).

4. Conclusioni

Per concludere, può affermarsi che, con la sentenza n. 170 del 2023, la Corte costituzionale ha segnato un precedente di indubbio rilievo, sanando quella che si era andata configurando come una vera e propria "zona franca" da ogni forma di garanzia in una materia delicata come quella della tutela delle comunicazioni private dei membri del Parlamento, protette dall'art. 68 Cost.
Non solo. La rilevanza della decisione risiede nel fatto che essa è destinata a dispiegare i suoi effetti ben al di là del caso da cui era originato il conflitto, estendendo le garanzie di cui all'art. 15 Cost. (in particolare, riserva di legge e di giurisdizione) ai mezzi di comunicazione interpersonale oggi più utilizzati dalla generalità dei cittadini, ossia quelli telematici. Di ciò la giurisprudenza dovrà necessariamente tenere conto.
Quanto, invece, allo schema procedurale applicabile alle ipotesi di sequestro di corrispondenza di membri del Parlamento, la scelta della Corte ha l'indubbio merito di fare chiarezza sull'interpretazione di una legge, la n. 140/2003, che, a ben vent'anni dalla sua approvazione, continua a far riflettere, ponendo quesiti non sempre di facile soluzione sia all'interprete che ai poteri dello Stato chiamati a darne applicazione.
Per tutte queste ragioni, la sentenza in commento è una di quelle decisioni destinate a "fare strada". E, sotto questo profilo, l'indicazione forse più significativa che si può trarre è la capacità del testo costituzionale, pur redatto in un periodo storico in cui strumenti come internet e le comunicazioni di natura telematica erano inimmaginabili, di adattarsi e continuare a fornire risposte ad una realtà in costante ed imprevedibile evoluzione.

Revirement dei giudici di merito: il direttore della testata telematica non risponde del reato di omesso controllo. Verso due nozioni di "stampa"?

Silvia Vimercati

Corte d'Appello di Milano, sez. III penale, 24 novembre 2022 (dep. 15 dicembre 2022), n. 7696

Il direttore di una testata telematica non risponde del reato di omesso controllo di cui all'art. 57 c.p. in quanto l'introduzione giurisprudenziale di una nozione più ampia di stampa può consentire l'estensibilità di norme di favore, ma – in assenza di un intervento del legislatore – non di fattispecie incriminatrici.

Sommario

Keywords

direttore testata telematica – responsabilità – Internet – stampa - omesso controllo

1. Il principio

Con la sentenza che si annota, la Corte d'Appello di Milano è tornata ad affrontare un tema che negli ultimi anni è al centro di una certo non lineare evoluzione giurisprudenziale: si tratta delle regole da applicare alle manifestazioni del pensiero in rete e, in particolare, della possibile estensione al web del regime specifico previsto per la carta stampata.

I giudici di merito milanesi, in contrasto con alcuni più recenti precedenti di legittimi-

[*] L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

tà, hanno stabilito che il direttore della testata telematica non può essere chiamato a rispondere del reato di cui all'art. 57 c.p.; norma che, come è noto, punisce a titolo di colpa per omesso controllo il direttore di un periodico cartaceo per i reati commessi per mezzo del giornale da lui diretto. E ciò in quanto la nozione evolutiva di "stampa" introdotta dalle Sezioni Unite nel 2015 – nozione che coincide con tutta l'informazione professionale, a prescindere dal mezzo con cui è diffusa – ben può giustificare l'estensione di norme favorevoli (quali le garanzie nei confronti del sequestro di cui all'art. 21 Cost), ma non può condurre all'applicazione di disposizioni sfavorevoli al di fuori dei casi tassativamente previsti in mancanza di una disciplina introdotta dal legislatore.

2. La vicenda

Anticipato l'esito della decisione e accennato al dibattito all'interno del quale essa si inserisce, pare opportuno soffermarsi in breve sul caso concreto.
Stando alla sintesi dei fatti offerta in motivazione, nel 2014 alcuni quotidiani online pubblicavano articoli offensivi nei confronti di un noto presentatore televisivo; più precisamente, diffondevano la notizia secondo la quale avrebbe sperperato i propri averi a causa di scommesse.
All'esito dell'udienza preliminare, il GUP del Tribunale di Milano dichiarava non luogo a procedere nei confronti degli imputati direttori delle testate online, escludendo che a costoro potesse essere applicato il reato di omesso controllo di cui all'art. 57 c.p. previsto esclusivamente per la stampa periodica tradizionale.
Avverso tale decisione proponeva appello il Pubblico Ministero, chiedendo di emettere decreto che dispone il giudizio per i reati di cui all'imputazione. La pubblica accusa, infatti, riteneva che le testate telematiche potessero essere ricondotte alla nozione di stampa di cui all'art. 1 l. 47/1948 e sottolineava che in più occasioni[1] la Corte di cassazione aveva affermato l'applicabilità del reato previsto dall'art. 57 c.p. anche al direttore di un giornale online.
La Corte d'Appello di Milano riformava parzialmente la sentenza impugnata dichiarando non doversi procedere solo in relazione a uno degli imputati per intervenuta remissione di querela dallo stesso accettata, mentre – per le ragioni già anticipate – la confermava nel resto, ribadendo l'inapplicabilità dell'art. 57 c.p. al direttore online.

3. Il precedente cammino della giurisprudenza di legittimità

Per apprezzare la portata (apparentemente) innovativa della sentenza in commento, occorre ripercorrere il cammino della giurisprudenza di legittimità in tema di estensione della responsabilità per omesso controllo al direttore della testata telematica.
Un primo indirizzo, univoco e a lungo mai smentito, riteneva che *de iure condito* al di-

[1] Per l'illustrazione di questo orientamento si veda il paragrafo terzo.

rettore di un giornale telematico non potesse estendersi il dettato dell'art. 57 c.p., così come non si potessero applicare ai fenomeni in rete tutte le altre disposizioni espressamente previste per la carta stampata.

Tale orientamento era stato inaugurato da una storica sentenza risalente al 2010[2], un *leading case* in materia, che aveva escluso l'applicabilità di tale fattispecie incriminatrice sulla base di due argomenti che paiono tuttora, come si dirà, convincenti.

In particolare, il primo consisteva nel divieto di analogia in *malam partem*, corollario del principio costituzionale di stretta legalità di cui all'art. 25, c. 2, Cost. La Cassazione prendeva le mosse dalla consapevolezza che la rete è un mezzo diverso dalla stampa e ciò perché il tenore letterale della definizione di stampa, contenuta all'art. 1 della l. 47/1948[3], non era in alcun modo suscettibile di ricomprendere i fenomeni presenti in rete. Data l'impossibilita di ricondurre le pubblicazioni online alla nozione di stampa, in forza del predetto principio costituzionale la soluzione non poteva che essere la seguente: la disposizione che punisce l'omesso controllo del direttore della stampa cartacea non era applicabile al direttore di un sito diffuso solo online.

Il secondo argomento si basava sull'impossibilità di muovere un rimprovero per una condotta di controllo, imposta dalla citata fattispecie incriminatrice, materialmente inadempibile da parte del direttore sui contenuti pubblicati in rete a fronte della natura interattiva della stessa. In altri termini, si riteneva che l'intrinseca eterogeneità del web avesse ricadute anche sul ruolo e sull'attività del direttore della testata telematica tali per cui un controllo come quello posto in essere dal direttore di un giornale cartaceo fosse in concreto inattuabile e quindi inesigibile.

Da qui, l'ulteriore passo compiuto dalla successiva giurisprudenza di legittimità: poiché alla nozione di "stampa" non potevano essere ricondotti i fenomeni che prendono corpo online, tutte le norme previste per il mezzo tradizionale – sia quelle di favore[4]

[2] Il riferimento è a Cass. pen., sez. V, 16 luglio 2010 (dep. 1° ottobre 2010), n. 35511, Brambilla, in *Diritto dell'informazione e dell'informatica*, 2010, 895 ss. La decisione è stata oggetto di numerosi commenti dottrinali, tra i quali: C. Melzi d'Eril, Roma locuta*: la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testata giornalistica* on line, in *Diritto dell'informazione e dell'informatica*, 2010, 899 ss.; N. Lucchi, *Internet, libertà di informazione e responsabilità editoriale*, in *Quaderni costituzionali*, 2011, 415 ss.; I. Salvadori, *La normativa penale della stampa non è applicabile,* de iure condito*, ai giornali telematici*, in *Cassazione penale*, 2011, 2982 ss.; S. Turchetti, *L'art. 57 c.p. non è applicabile al direttore del periodico online*, in *penalecontemporaneo.it*, 17 novembre 2010.

[3] Secondo la definizione contenuta nell'art. 1 l. 47/48 per stampa si intendono «tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubblicazione».

[4] In merito alla applicabilità delle disposizioni di favore, nel 2014 la Corte di Cassazione aveva statuito che le garanzie costituzionali previste per gli stampati in tema di sequestro non potessero essere estese agli spazi comunicativi virtuali. Il riferimento è a due decisioni emesse entrambe dalla V sezione a distanza di pochi giorni: la prima, Cass. pen., sez. V, 5 novembre 2013 (dep. 5 marzo 2014), n. 10594, in *dirittopenalecontemporaneo.it*, 25 marzo 2014, con nota di C. Melzi d'Eril, *La Cassazione esclude l'estensione delle garanzie costituzionali previste per il sequestro degli stampati*; la seconda, Cass. pen., sez V, 30 ottobre 2013 (dep. 12 marzo 2014), n. 11895, in *medialaws.eu*, con nota di F. Mazara Grimani, *Il sequestro preventivo di un blog: nuovi orientamenti alla luce della sentenza della Corte di Cassazione n. 11895/2014*. Per un puntuale commento critico di entrambe le decisioni, si v. C. Melzi d'Eril, *Il sequestro dei siti on-line: una proposta di applicazione analogica dell'art. 21 Cost. "a dispetto" della giurisprudenza*, in *Diritto dell'informazione e dell'informatica*, 2014, 153 ss.

sia le disposizioni penali sfavorevoli[5] – non erano applicabili alla rete internet.
Come si è visto, il riconoscimento della intrinseca diversità tra stampa e internet era il presupposto indefettibile dell'argomentazione principale, ossia il divieto di analogia in materia penale, che aveva condotto a negare che l'attività del direttore della testata telematica potesse essere ricondotta nell'alveo della fattispecie di cui all'art. 57 c.p[6].
Senonché, una decisione delle Sezioni Unite del 2015, pur intervenendo su una questione differente, ossia la possibile estensione delle guarentigie costituzionali previste dall'art. 21 Cost. per la stampa, aveva posto le basi per il successivo mutamento di tale consolidato approdo.
Per quel che qui interessa, con sentenza n. 31022 del 2015[7] la Cassazione ha avuto

[5] Per quanto riguarda le norme di sfavore, oltre al reato di cui all'art. 57 c.p., e sempre in forza del divieto di analogia in *malam partem*, era stata esclusa l'applicabilità dell'aggravante prevista dall'art. 13 della legge stampa, nonché del reato di stampa clandestina di cui all'art. 16 della medesima legge. Sull'inestensibilità alla rete dell'art. 13 l. 47/48, tra le molte, si veda Cass. pen., sez. V, 1 febbraio 2017, n. 4873 in *Quotidiano del Diritto,* 2 febbraio 2017, con nota di A. Galimberti, *Diffamazione "attenuata" se via Fb;* in *penalecontemporaneo.it*, 20 aprile 2017, E. Birritteri, *Diffamazione e Facebook: la Cassazione conferma il suo indirizzo ma apre a un'estensione analogica in malam partem delle norme sulla stampa*; in *Forum di Quaderni Costituzionali*, 14 aprile 2017, con nota di M. Tresca, *Il diritto di informazione nell'era digitale: la complessa equiparazione tra stampa tradizionale e media on line*; nonché, volendo C. Melzi d'Eril-S. Vimercati, *Diffamazione, Facebook non è stampa*, in *Il Sole 24 Ore online*, 8 febbraio 2017; va comunque segnalato che, alla luce di Corte cost., 12 luglio 2021, n. 150 (che ha dichiarato illegittima la norma in esame) la questione è oggi superata. Sull'inapplicabilità del reato di stampa clandestina di cui all'art. 16 della l. 47/1948 a un blog non registrato si veda Cass. pen., sez. III, 10 maggio 2012, n. 23230, in *penalecontemporaneo.it*, 8 ottobre 2012, con nota di F. Piccichè, *Giornali on line e reato di stampa clandestina*; in *Diritto dell'informazione e dell'informatica*, 2012, 1118, con nota di P. Di Fabio, *Blog, giornali on line e «obblighi facoltativi» di registrazione delle testate telematiche: tra confusione del legislatore e pericoli per la libera espressione del pensiero su internet*.

[6] Nello stesso senso della sentenza cd. Brambilla del 2010, si era espressa poco dopo la Cassazione ribadendo la non configurabilità del reato di omesso controllo nei confronti del direttore di un giornale online: si tratta di Cass. pen., sez. V, 28 ottobre 2011 (dep. 29 novembre 2011), n. 44126, Hamaui, in *Diritto dell'informazione e dell'informatica*, 2011, 795 con nota di G. E. Vigevani, *La «sentenza figlia» sul direttore del giornale telematico: il caso Hamaui*; più di recente, Cass. pen., sez. V, 21 novembre 2017 (dep. 19 febbraio 2018), n. 7885, con cui la Corte, seppur in *obiter dictum*, ha avuto occasione di riaffermare che all'informazione on line non è applicabile l'art. 57 c.p. Nello stesso senso, anche Cass. pen., sez. V, 28 settembre 2017 (dep. 20 novembre 2017), n. 52743, in *Diritto Penale Contemporaneo*, 6, 2018, 125 ss., con nota di E. Pietrocarlo, *Concorso in diffamazione del direttore e articolo firmato con pseudonimo: la Cassazione insiste sulla responsabilità "di posizione"*, ove la Cassazione, ha stabilito che, in caso di articolo anonimo o firmato con uno pseudonimo, il direttore può essere chiamato a rispondere di concorso in diffamazione *ex* artt. 110 e 595, c. 3, c.p. se sulla base di circostanze esteriori siano accertati il consenso o la meditata adesione dello stesso al contenuto dello scritto, ma – aderendo al consolidato orientamento della giurisprudenza di legittimità – non del reato di omesso controllo perché l'attività on line non può essere ricondotta nel concetto di stampa periodica. Per un commento ulteriore a quest'ultima decisione si veda altresì A. Trimarchi, *La responsabilità (ancora una volta oggettiva) del direttore di periodico* online *per l'articolo diffamatorio con pseudonimo anonimizzante*, in questa *Rivista*, 3, 2018, 254 ss.

[7] Cass., sez. un., 29 gennaio 2015 (dep. 17 luglio 2015), n. 31022, in *penalecontemporaneo.it*, 9 marzo 2016, con nota di C. Melzi d'Eril, *Contrordine compagni: le Sezioni Unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate on-line registrate*; in *Quaderni costituzionali*, 2015, 1013 ss., con nota di P. Caretti, *La Cassazione pone, meritoriamente, alcuni punti fermi in tema di regolazione dell'informazione via internet*; in *Processo penale e giustizia*, 2015, 78, con nota di A. Pulvirenti, *Sequestro e Internet: dalle Sezioni Unite una soluzione equilibrata ma "creativa"*; in *Cassazione penale*, 2015, 3454 ss., con nota di L. Paoloni, *Le Sezioni Unite si pronunciano per l'applicabilità alle testate telematiche delle garanzie costituzionali sul sequestro della stampa:* ubi commoda, ibi et incommoda*?*; in *medialaws.eu*, 17 maggio 2016, con nota di A. Regi, *Le Sezioni Unite si pronunciano sull'applicabilità delle garanzie costituzionali in tema di sequestro preventivo alle testate telematiche registrate*; in *Guida al diritto*, 2015, 38, 82 ss., con nota di C. Melzi d'Eril-G. E. Vigevani, *Il sequestro di una pagina web può essere disposto imponendo al service provider di renderla inaccessibile*; in *Diritto penale e processo*, 2015,

l'occasione di offrire una nuova definizione del termine "stampa". In particolare, secondo le Sezioni Unite era necessario attribuire alla nozione di stampa un differente significato, che fosse coerente con il progresso tecnologico e le mutate abitudini del pubblico: essa, intesa in senso "figurato", corrisponderebbe all'informazione giornalistica professionale, sia se diffusa su carta stampata che attraverso il web.

La necessità di offrire un'interpretazione estensivo-evolutiva del concetto di stampa nasceva dalla situazione di tensione con il principio di uguaglianza determinata dall'irragionevole differenza di trattamento dell'informazione veicolata su carta stampata rispetto a quella diffusa in rete: soltanto la seconda, non beneficiando delle garanzie previste dall'art. 21 Cost. per la stampa, sarebbe stata assoggettabile a sequestro preventivo per le ipotesi di diffamazione. In altri termini, a detta della Cassazione, si correrebbe il rischio di porre in essere trattamenti differenziati a due fattispecie, cioè giornali online e cartacei, assai simili sotto il profilo funzionale di diffusione dell'informazione professionale.

Proprio grazie all'individuazione di tale nuovo concetto di stampa, le Sezioni Unite hanno stabilito che i giornali online registrati, in quanto coincidenti sotto i profili strutturale e funzionale a quelli tradizionali, sono soggetti alla normativa ordinaria e costituzionale specificatamente prevista per i secondi e beneficiano pertanto delle garanzie costituzionali in materia di sequestro preventivo.

L'innovativa interpretazione della nozione di stampa e il conseguente principio di diritto espresso dalle Sezioni Unite, prima in sede penale e poi a distanza di breve tempo anche in sede civile[8], hanno rappresentato la premessa per un radicale cambio di posizione della giurisprudenza anche con riferimento all'ambito di applicazione del reato di omesso controllo di cui all'art. 57 c.p.

Dopo tali pronunce, a partire dal 2018 le sezioni semplici hanno infatti cominciato a smentire il proprio precedente orientamento, affermando che ai giornali online, proprio perché ora ritenuti riconducibili alla nuova nozione di stampa, dovessero applicarsi le disposizioni incriminatrici previste per la carta stampata, tra cui appunto il reato di omesso controllo[9].

2002, con nota di S. Lorusso, *Un'innovativa pronuncia in tema di sequestro preventivo di testata giornalistica on line*; in *Diritto dell'informazione e dell'informatica*, 2015, 1041 ss., con nota di G. Corrias Lucente, *Le testate telematiche registrate sono sottratte al sequestro preventivo. Qualche dubbio sulla "giurisprudenza legislativa"*.

[8] L'anno successivo tale approdo è stato accolto anche dalle Sezioni Unite civili, le quali hanno statuito che le norme di favore in tema di sequestro previste per la stampa si applicano al giornale online quando quest'ultimo presenti le caratteristiche del giornale cartaceo, ovverosia una testata, un direttore responsabile, una redazione e un editore: v. Cass. civ., Sez. Un., 25 ottobre 2016 (dep. 18 novembre 2016), n. 23469, in *Diritto dell'informazione e dell'informatica*, 2016, 706 ss.

[9] La prima decisione ad affermare l'estensibilità dell'art. 57 c.p. al direttore della testata telematica, a quanto consta, è Cass. pen., sez. V, 11 dicembre 2017 (dep. 22 marzo 2018), n. 13398. Per un commento, volendo, S. Vimercati, *Il* revirement *della Cassazione: la responsabilità per omesso controllo si applica al direttore della testata telematica*, in questa *Rivista*, 2, 2018, 324 ss. Nello stesso senso, successivamente, tra le molte, Cass. pen., sez. V, 12 gennaio 2021, n. 7220.

4. La motivazione della Corte d'appello di Milano

Il percorso motivazionale che ha portato la Corte d'appello di Milano a escludere l'applicabilità del reato di omesso controllo al direttore di un giornale telematico si pone in aperto contrasto con tale più recente indirizzo della giurisprudenza di legittimità e, viceversa, risulta allineato all'orientamento cristallizzato in precedenza a cui espressamente aderisce e del quale vengono accolte le argomentazioni e l'impianto ermeneutico.

Per giungere a tale conclusione, i giudici meneghini individuano subito quale chiave di volta l'interpretazione del concetto di stampa e la sua (mancata) evoluzione a livello normativo.

Anzitutto viene ricordato l'orientamento di legittimità accolto dal 2010 che, come si è detto, negava l'estensibilità dell'art. 57 c.p. muovendo dalla riconosciuta eterogeneità tra stampa tradizionale e informazione telematica e dalla impossibilità di ricondurre la seconda alla definizione contenuta all'art. 1 l. 47/48. Dopodiché la Corte richiama l'innovativa sentenza delle Sezioni Unite del 2015 che, introducendo la nuova nozione evolutiva di stampa che si è sopra richiamata, tale da ricomprendere tutta l'informazione professionale, aveva sostanzialmente parificato quella veicolata con periodici cartacei e quella diffusa con giornali telematici.

Proprio da qui, secondo la Corte d'appello, sarebbe derivato l'errore in cui sarebbe incorsa la giurisprudenza successiva: e cioè ritenere applicabili non solo le garanzie (nello specifico quelle previste in tema di sequestro dall'art. 21 Cost.) ma anche le disposizioni incriminatrici previste espressamente solo per la stampa e, in particolare, allargare la fattispecie di cui all'art. 57 c.p. pur in assenza di un intervento normativo. Per tale ragione, con parole che non lasciano spazio a dubbi di sorta, viene sottolineato che «il tentativo di interpretazione estensiva delle Sezioni Unite, avvenuto per tutelare il contenuto dell'attività giornalistica, è divenuta definitiva analogia in *malam partem* per le operazioni ermeneutiche della giurisprudenza successiva».

Proprio perché nei precedenti più immediati di legittimità il nodo della questione si è giocato su un'interpretazione pericolosamente in bilico fra estensione e analogia, la Corte d'Appello ha utilmente voluto ribadire la pur nota differenza tra interpretazione estensiva, ossia un procedimento argomentativo che resta situato all'interno del significato letterale della disposizione, e analogia, che presuppone invece il superamento della lettera della legge e consiste nell'applicare a un caso non espressamente regolato dalla legge una norma che disciplina un'ipotesi simile; e, come noto, la seconda operazione interpretativa, a differenza della prima, in virtù dell'art. 14 delle Preleggi e più in generale dell'art. 25 Cost. è vietata per le leggi penali.

Il riferimento alla distinzione tra i due criteri di auto-integrazione del diritto, l'interpretazione estensiva e quella analogica, introduce il passaggio successivo della motivazione: secondo la Corte d'appello, l'interpretazione estensiva del concetto di stampa compiuta dalle Sezioni Unite nel 2015 deve ritenersi legittima perché volta a estendere norme di favore, ossia le garanzie in tema di sequestro preventivo di cui all'art. 21 Cost.; viceversa, l'automatica estensione dello statuto penale previsto per la stampa non può trovare cittadinanza nel nostro ordinamento perché, in materia penale, l'in-

terprete non ha il potere di colmare quelli che egli percepisce quali vuoti normativi, applicando analogicamente disposizioni incriminatrici e così di fatto creando nuove fattispecie di reato al di là di quanto espressamente stabilito dal legislatore.
Di qui, l'affermazione secondo cui la giurisprudenza delle sezioni semplici successiva alla pronuncia del 2015 avrebbe violato il divieto di analogia in *malam partem*, ritenendo che l'applicazione del reato di cui all'art. 57 c.p. anche al direttore del giornale on line si ponga al di là di quanto previsto e quanto desumibile dal testo della disposizione.
In conclusione, all'esito del percorso ermeneutico di cui si è dato conto, i giudici milanesi, parlando in modo per nulla sibillino, rilevavano che «se davvero un'esigenza di responsabilizzazione per omesso controllo esiste, anche nel settore telematico, è solo il legislatore che può legittimamente farsene carico. Ad oggi, in assenza di una previsione normativa in questo senso, non è compito del giudice colmare un vuoto normativo con l'applicazione analogica di una previsione punitiva».

5. Qualche considerazione conclusiva

Dato conto dell'evoluzione giurisprudenziale e reso noto il contenuto della motivazione della sentenza in commento, merita ora svolgere alcune riflessioni sul percorso interpretativo e sugli argomenti che hanno condotto la Corte a (ri)affermare l'inapplicabilità del delitto previsto dall'art. 57 c.p. al direttore della testata telematica.
Le cifre fondamentali di questa decisione, che ne marcano l'importanza, paiono il rigore ermeneutico e la forza delle argomentazioni.
Quale sia il punto di arrivo dei giudici milanesi lo si è già precisato: l'inedita nozione di stampa introdotta in via giurisprudenziale dalle Sezioni Unite nel 2015 consente l'estensione di norme di favore, ma non può giustificare l'applicabilità di fattispecie incriminatrici, in assenza di un intervento normativo, pena la violazione del divieto di analogia in *malam partem*.
Per giungere a tale esito – che, lo si afferma fin d'ora, si ritiene del tutto condivisibile – la Corte si è mossa all'esplicito fine di non incorrere in una violazione dei principi fondanti del diritto penale. Di qui, individuando con precisione la linea di confine tra interpretazione estensiva, consentita, e interpretazione analogica *in malam partem*, vietata, in materia penale, ha (opportunamente) ritenuto che la giurisprudenza di legittimità che aveva applicato il reato di omesso controllo anche al direttore del quotidiano online avesse violato il divieto di interpretazione analogica.
Tale indirizzo sull'ambito di applicazione dell'art. 57 c.p. accolto dal 2018 era stato presentato come la piana conseguenza di quanto statuito dalle Sezioni Unite; sembrava infatti darsi per scontato che la nozione di stampa contenuta nell'art. 57 c.p. e quella di cui all'art. 1 della l. 47/48 fossero del tutto sovrapponibili a quella dell'art. 21 Cost.
Viceversa, la sentenza in esame, muovendo dal presupposto che l'equiparazione tra giornali cartacei e online era stata introdotta in un procedimento in cui di discuteva solo dell'estensione delle guarentigie costituzionali, ha il pregio di aver posto un argine alla nuova nozione di stampa: limitarla solo a casi analoghi di applicazione delle disposizioni di favore contenute nell'art. 21 Cost. ed evitare di ritenerla estesa all'intero

ordinamento, in modo tale da non conferirle una portata generale che implicherebbe l'applicabilità anche delle disposizioni di sfavore. Queste ultime, infatti, devono essere interpretate in modo restrittivo, nel pieno rispetto dei principi di tassatività e legalità, che dovrebbero far prediligere l'interpretazione letterale ad ogni altro criterio esegetico. A ben vedere, peraltro, in Costituzione esistono molte espressioni che sono di norma interpretate attribuendo loro un significato in parte o del tutto diverso da quello che assumono nella legislazione ordinaria; si pensi ad esempio alla nozione costituzionale di buon costume che è diversa da quella utilizzata nel codice civile e nel codice penale. Di conseguenza, se le Sezioni Unite hanno in effetti introdotto una nuova nozione di stampa, apposta per l'art. 21 Cost., ciò non deve far trarre la conseguenza che esista una e una sola nozione di stampa, valida sia per l'art. 21 Cost., sia per la legge n. 47/48 e per le disposizioni del codice penale. E così, ben potrebbe ritenersi che possano esistere due distinte nozioni di stampa, una per l'articolo 21 e l'altra per la legge 47/48, lasciando così impregiudicato il significato che tale parola assume per le disposizioni del codice penale e in altri testi della legislazione ordinaria. In altri termini, per stampa potrebbe intendersi l'informazione di tipo professionale quando l'espressione è contenuta in Costituzione – il che consente di estendere le garanzie in materia di sequestro anche ai giornali telematici – mentre potrebbe continuare a indicare le sole riproduzioni cartacee quando la medesima espressione si rinviene in disposizioni di rango primario, circostanza che eviterebbe di ampliarne l'estensibilità e di incorrere in una violazione del principio di legalità in materia penale.

Anche per queste ragioni, non può che condividersi la valutazione critica dei giudici milanesi sul percorso logico-giuridico della più recente giurisprudenza di legittimità; esso, in effetti, pareva sganciato dai criteri interpretativi rigorosi che presidiano l'applicazione delle disposizioni penali e si esponeva alla critica di porsi al di là del ruolo nomofilattico riconosciuto alla Cassazione, per aver proposto un'interpretazione dell'art. 57 c.p. talmente disancorata dal testo da scivolare verso la funzione legislativa.

In conclusione, la forza degli argomenti e il modo perentorio in cui la Corte di Milano si è espressa lasciano la sensazione di un – assai opportuno – ritorno al passato e la speranza che in futuro anche la giurisprudenza di legittimità torni sui propri passi. E ciò perché si continua a ritenere che, allo stato, solo il legislatore in quanto unico soggetto cui compete individuare l'area del punibile, cosicché ai cittadini sia garantita la prevedibilità dei precetti penali, potrebbe imporre una qualche forma di controllo al direttore on line, assistita da una sanzione penale; tuttavia, in assenza di un simile intervento normativo che introduca disposizioni testuali concepite per la rete, e dunque adeguate alle sue caratteristiche e alle condotte che materialmente si possono chiedere agli operatori on line, destano inevitabilmente perplessità i tentativi di allargare l'area del penalmente rilevante a fenomeni che non sono riconducibili al dettato delle disposizioni incriminatrici.

Cronache

Intelligenza Artificiale generativa: alcune questioni problematiche*

Marco Bassini

Sommario

1. Introduzione

L'avvento su larga scala dei sistemi di Intelligenza Artificiale c.d. "generativa", attestatosi in tempi rapidissimi su un livello di capillarità e crescita senza precedenti, ha dato nuova linfa un dibattito già assai partecipato sulla necessità di una regolamentazione a prova di futuro. Invero, proprio i facili entusiasmi che taluni avevano coltivato salutando la scelta delle istituzioni dell'Unione europea di avviare un processo volto a coniare un quadro normativo *ad hoc* (l'AI Act) sembrano ora aver subito una tappa d'arresto a fronte delle difficoltà di tenere il passo dello sviluppo tecnologico. Queste carenze trovano una manifestazione evidente, del resto, nell'iter legislativo dell'AI Act, che ha visto il Consiglio e il Parlamento europeo tentare non senza fatica di rimediare "in corso d'opera" all'assenza di regole che potessero cogliere e affrontare le peculiarità dell'Intelligenza Artificiale generativa nel testo originale proposto dalla Commissione.
Questo intervento si diffonderà anzitutto sui profili di carattere generale inerenti all'ipotesi di una disciplina dell'Intelligenza Artificiale generativa, per poi concentrarsi, senza alcuna pretesa di esaustività, su alcuni punti nevralgici particolari che allo stato caratterizzano, nel settore dei media, il posizionamento di questa tecnologia.

* Il testo riproduce il contenuto della relazione svolta al convegno "Pluralismo e diritto d'autore al tempo dell'intelligenza artificiale" organizzato dall'Italian Chapter dell'International Institute of Communications in collaborazione con l'Autorità per le garanzie nelle comunicazioni, in Roma, 21 settembre 2023.

2. Profilo generale: la difficile costruzione di un quadro giuridico

La volontà delle istituzioni dell'Unione europea di restituire, con l'AI Act, un assetto giuridico adeguato alla complessità e poliedricità della tecnologia merita sicuro apprezzamento e in questo quadro l'intervento di natura "adeguatrice" che tanto Consiglio quanto Parlamento hanno proposto si segnala come uno sforzo encomiabile. Tale valutazione riesce peraltro corroborata dalla considerazione del fattore temporale che caratterizzerà la messa a regime prima e l'attuazione poi del nuovo quadro normativo, non destinato a una traduzione in pratica immediata (un tema su cui forse l'Unione europea dovrebbe interrogarsi, alla luce dell'estensione del suo intervento nell'ambito digitale negli ultimi anni). Se il disegno di aggiornamento merita condivisione, si deve tuttavia notare come la garanzia di certezza giuridica non possa passare per il tramite di una sostanziale giustapposizione di norme, come quella che il testo approvato dal Consiglio e quello licenziato dal Parlamento sembrerebbero proporre. La missione delle istituzioni non è certamente, del resto, quella di *filling the gap*; ma semmai quella di tracciare un delicato equilibrio tra le diverse istanze che ruotano intorno all'avvento e alla diffusione su larga scala dei sistemi di Intelligenza Artificiale. In questo senso, le norme di cui i testi di Parlamento e Consiglio propongono l'adozione con riferimento ai modelli generativi paiono non del tutto convincenti, in quanto traducono un approccio incentrato non tanto sulla disciplina dell'utilizzo della tecnologia in questione quanto sulla tecnologia *tour court*. Riaffiora, in questo frangente, traccia dell'ansia regolatoria che contraddistingue molti legislatori a fronte dell'innovazione tecnologica. Un intervento regolamentare così esclusivamente calibrato sulla tecnologia "in quanto tale", insensibile e indifferente invece agli utilizzi particolari, potrebbe del resto trovare giustificazione soltanto sull'assunto di una intrinseca quanto indimostrata sua "pericolosità". Questo approccio si rivelerebbe oltremodo inesatto se applicato all'Intelligenza Artificiale, specialmente *general purpose*, e ai c.d. modelli fondazionali, dove la possibilità di definire il livello di rischio e correlarlo alla tecnologia è *in re ipsa* sconfessata dalla pluralità e varietà di contesti di utilizzo *downstream*. Questa considerazione è corroborata, peraltro, dalle riflessioni già presenti in letteratura sulla difficoltà di costringere i sistemi di Intelligenza Artificiale generativa entro il rigido schema precostituito dall'AI Act e fondato su livello di rischio. Tali criticità hanno fatto ipotizzare, con riflessioni che parrebbero condivisibili, l'opportunità di ideare una categoria di rischio *ad hoc*, congegnata alla luce delle caratteristiche peculiari dei modelli fondazionali e dell'Intelligenza Artificiale generativa, e così slegata dalla preconcetta elaborazione racchiusa nelle categorie delineate dall'AI Act. Tale soluzione assicurerebbe maggiore flessibilità e promette di cogliere in modo più accurato il rischio insito in questa categoria tecnologica meritevole di una considerazione autonoma. L'argomento del superamento delle categorie di rischio individuate dall'AI Act avendo senz'altro a mente perlopiù l'Intelligenza Artificiale *special purpose* non può essere peraltro trascurato, a fronte delle significative implicazioni concorrenziali che si ricollegano all'apparato di obblighi derivante dell'AI Act. Allo stato, sebbene sembri scongiurato il pericolo di una pedissequa equiparazione dell'Intelligenza Artificiale generativa ai sistemi a rischio elevato (come invece nel te-

sto votato dal Consiglio), il reticolato normativo costruito intorno a questa tecnologia sembrerebbe farne *sostanzialmente* dei sistemi di tale natura. Trattare l'Intelligenza Artificiale generativa come la tecnologia più rischiosa, oltre probabilmente a non rifletterne accuratamente le caratteristiche, è operazione che – come accennato – non è immune da conseguenze sul piano concorrenziale: elevato è, infatti, il pericolo che a poter rispondere dei gravosi obblighi imposti agli operatori di questo segmento di mercato, e in particolare a fornitori e sviluppatori, siano nei fatti soltanto gli attori imprenditoriali più strutturati e dotati di copertura finanziaria, con inevitabili ripercussioni sul piano dello sviluppo dell'innovazione e del possibile ingresso di nuovi *player* nel mercato, che riuscirebbe con ogni probabilità scoraggiato.

3. La qualità dei dati come premessa per la generazione legale di contenuti (*passim*)

Passando ai profili particolari, un tema occupa una posizione nevralgica rispetto a tutte le questioni che, tanto nella prospettiva dei dati quanto in quella dei contenuti, emergono dallo sviluppo dell'Intelligenza Artificiale generativa: la qualità dei dati. Non è un caso che le problematiche principali, già denunciate da diversi commentatori, derivino vuoi dalla generazione di output contenutisticamente errati, che risalgono a informazioni inesatte magari perché non più attuali (le c.d. "allucinazioni"), vuoi dalla memorizzazione di informazioni a carattere personale che vengono "randomicamente" riproposte, talvolta senza alcun legame con l'oggetto dell'attività generativa. In termini di trattamento di dati e di elaborazione di contenuti si pone un comune problema di qualità dei dati, funzionale a evitare l'automatismo *garbage in, garbage out*. Si tratta di un nodo che non riguarda soltanto l'ambito del trattamento di dati personali (al quale è comunque affrancato dal principio di esattezza dei dati racchiuso nel GDPR, tra gli altri) ma che è foriero di significative implicazioni anche sul piano dei contenuti. Non è casuale che in letteratura si sia già sollevata, opportunamente, una riflessione in ordine all'opportunità di dettare specifiche garanzie a tutela dalla qualità dei dati, prescindendo dai rimedi già esistenti (ritenuti insufficienti) nella normativa sulla protezione dei dati.

4. L'applicabilità delle esenzioni di responsabilità per i fornitori di servizi digitali alle creazioni dell'Intelligenza Artificiale generativa

Svolta la doverosa premessa affidata al paragrafo che precede, è doveroso domandarsi quale sia l'impatto dell'Intelligenza Artificiale generativa sul quadro normativo inerente ai servizi digitali che di recente è stato confezionato dalle istituzioni dell'Unione europea, con l'adozione in particolare del Digital Services Act ("DSA", regolamento (UE) 2022/2065) e del Digital Markets Act ("DMA", regolamento (UE) 2022/1925). Prescindendo in questa sede dall'esame dei profili concorrenziali (senza tacere però la loro rilevanza e anticipando che criticità emergono anche rispetto all'applicazione del DMA

ai sistemi di Intelligenza Artificiale generativa), l'esigenza di considerare le norme contenute nel DSA trae origine dalla temuta capacità della tecnologia in discorso di produrre e disseminare non soltanto contenuti illeciti ma anche (e soprattutto) contenuti falsi (tra cui, per esempio, i c.d. *deepfakes*). Proprio la capacità dell'Intelligenza Artificiale generativa a prestarsi per questi scopi è all'origine delle preoccupazioni inerenti a un suo possibile uso per alimentare campagne d'odio o disinformative che potrebbero tradursi in effetti distorsivi sul piano democratico. Proprio il DSA è stato celebrato, forse con enfasi talvolta eccessiva, come il risultato di un profondo ammodernamento del quadro giuridico applicabile ai servizi digitali reso ormai necessario dalla conclamata obsolescenza della Direttiva sul commercio elettronico (direttiva 2000/31/CE). Come noto, quest'atto fa propria una matrice regolamentare già comune ad altre normative presenti (come il GDPR) e future (come l'AI Act), ossia l'approccio basato sul rischio. Addiviene a una differenziazione e specificazione a lungo attesa degli obblighi e delle misure di contrasto dei rischi che è calibrata sul tipo di servizio erogato e sul livello di rischio inerente. Proprio per questo, la riforma è stata salutata come un momento di svolta che impone alle piattaforme online di dimensioni elevate (c.d. VLOP, *very large online platforms*), tra cui i social network, obblighi più stringenti, anche in tema di trasparenza, rispetto alla moderazione di contenuti di terzi. Questo importante traguardo sembrerebbe però frustrato dall'avvento di un *novum* in grado di bypassare, almeno all'apparenza, le maglie delle prescrizioni esistenti.

È del tutto evidente che i modelli di Intelligenza Artificiale generativa non erano presenti alla mente del legislatore del DSA: non lo erano, del resto, nemmeno a quella del legislatore dell'AI Act che ha confezionato la proposta della Commissione. Parrebbe dunque inevitabile riconoscere che l'articolata trama normativa ora racchiusa nel regolamento non possa trovare applicazione rispetto alla creazione di contenuti derivanti dall'Intelligenza Artificiale generativa. Si badi: il DSA sarebbe comunque applicabile a tali contenuti quanto pubblicati da terzi su piattaforme online di grandi dimensioni, come un social network, o attraverso altri servizi che ricadono nell'ambito di applicazione del regolamento. Ciò che resterebbe esclusa è, invece, l'applicazione delle norme in questione agli sviluppatori o utilizzatori di Intelligenza Artificiale generativa. Per fare un esempio immediato: ChatGPT non potrebbe invocare alcuna esenzione di responsabilità rispetto ai contenuti generati.

Nonostante questa opinione dominante sia suffragata dalle intenzioni del legislatore, vi è in dottrina una tesi finora minoritaria che, pur riconoscendo che il DSA non è stato pensato perché trovasse applicazione ai sistemi di Intelligenza Artificiale generativa e ai soggetti della relativa *value chain*, ha evidenziato come sussisterebbero delle "pieghe" nel testo del regolamento che potrebbero giustificare una sua estensione anche oltre il perimetro dei servizi digitali come tradizionalmente identificati. Questo spazio interpretativo è stato ricavato dalla nozione dei motori di ricerca online fatta propria dal DSA. Si tratta, come noto agli addetti ai lavori, di una categoria "in cerca d'autore", che nel silenzio serbato dalla Direttiva sul commercio elettronico ha conosciuto declinazioni normative diverse tra gli Stati membri. Il DSA racchiude una definizione analoga a quella precedente, secondo cui è motore di ricerca online «un servizio intermediario che consente all'utente di formulare domande al fine di effettuare

ricerche, in linea di principio, su tutti i siti web, o su tutti i siti web in una lingua particolare, sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, richiesta vocale, frase o di altro input, e che restituisce i risultati in qualsiasi formato in cui possono essere trovate le informazioni relative al contenuto richiesto» (così l'art. 3, par. 1, lett. j) del DSA). Per effetto dell'adesione a questa definizione sarebbe possibile riscontrare alcuni punti di contatto tra la categoria dei motori di ricerca online e perlomeno alcuni sistemi di Intelligenza Artificiale generativa. Entrambi (motori di ricerca e sistemi di Intelligenza Artificiale generativa), infatti, fonderebbero il proprio funzionamento sull'input inziale (*prompt*) dei propri utenti, teso alla ricerca di informazioni sul web sulla base della parola chiave utilizzata. Entrambi, poi, sarebbero in grado di restituire i risultati *in qualsiasi formato* in cui possono essere trovate le informazioni relative al contenuto richiesto. E proprio su questo carattere di indifferenza rispetto alle modalità con cui il sistema restituirebbe il risultato desiderato dagli utenti fa perno l'interpretazione che vuole come possibile la riconduzione di alcuni sistemi di Intelligenza Artificiale generativa alla categoria dei motori di ricerca online, con conseguente possibilità di sottoporli alle regole previste per i VLOSE, ossia i *very large online search engines.*
La tesi che si è esposta poggia su un fragile elemento di ambiguità letterale e può essere avversata semplicemente richiamando la volontà del legislatore di dedicare il quadro normativo a una tipologia ben determinata di servizi digitali. Nondimeno, proprio la lettura audacemente proposta che è stata ora richiamata stimola la riflessione su un punto di auspicabile avanzamento del dibattito: l'applicazione del DSA agli sviluppatori di sistemi di Intelligenza Artificiale generativa sarebbe auspicabile?
A ben vedere, questa operazione, se perfezionata tramite un apposito disegno di riforma, potrebbe condurre a due risultati pratici non trascurabili.
Da un lato, dall'applicazione del DSA discenderebbe l'operatività dell'esenzione di responsabilità prevista per i fornitori di servizi allo stato assoggettati al regolamento. Un simile esito potrebbe apparire paradossale a chi ritenga che la creazione di output come testi, video o immagini sia equiparabile e indicativa di una attività editoriale e così dubitare delle ragioni per un regime giuridico che diverga dalle ordinarie regole in tema di allocazione di responsabilità per contenuti illeciti. Nondimeno, proprio nel contesto di un'attività generativa che abbisogna di continuo addestramento a fronte della possibilità di errori (allucinazioni?) pare che il sistema di *notice and action* che il DSA ha ereditato e rimodellato dalla Direttiva sul commercio elettronico ben si presti ad assolvere questa missione. Segnalando un contenuto illecito (o comunque inappropriato) agli sviluppatori di sistemi di Intelligenza Artificiale generativa, infatti, si potrebbe favorire un intervento sul processo che ha determinato la restituzione di un risultato non conforme all'ordinamento giuridico, al contempo delimitando il margine di applicazione dell'esenzione di responsabilità, che non potrebbe estendersi "oltre" il momento in cui sia stata portata a conoscenza l'illiceità del risultato generato. Ne gioverebbe, forse, anche la certezza del diritto.
Dall'altro lato, l'estensione delle regole contenute nel DSA, come è stato notato da chi ha proposto la tesi sopra richiamata, potrebbe favorire l'applicazione, perlomeno ai soggetti maggiormente strutturati (onde evitare conseguenze anticoncorrenziali) di più elaborati meccanismi di valutazione del rischio come quelli indicati all'art. 34 DSA. In

questo modo, peraltro, l'estensione del DSA risolverebbe forse un problema al legislatore dell'AI Act, impegnato nella faticosa ricerca di un punto di equilibrio.
Lo stesso problema potrebbe porsi, poi, negli Stati Uniti, laddove hanno peraltro sede numerosi attori imprenditoriali operativi anche in Europa. In questo senso, l'attuale schema della Section 230 del Communications Decency Act parrebbe non lasciare spazio ad alternative tra la qualificazione degli sviluppatori e fornitori di sistemi di Intelligenza Artificiale generativa come *information service provider* e *information content provider,* con quest'ultima opzione qualificatoria verosimilmente candidata – in assenza di interventi legislativi – a trovare supporto in eventuali contenziosi avanti alle corti statunitensi. L'*impasse* sull'opportunità di una riforma della Section 230 CDA si prolunga ormai da tempo e il dibattito potrebbe essere forse l'occasione per un suo superamento. Del resto, anche aderendo all'impostazione che ravvisa – non senza ragioni – negli attori in questione *information content provider*, vi sarebbe spazio per discutere l'opportunità delle conseguenze giuridiche (in termini di esclusione dell'esenzione di responsabilità in bianco accordata per contenuti diffamatori).

5. La riconducibilità dei prodotti di Intelligenza Artificiale generativa a tutela costituzionale

Vi è poi un convitato di pietra nel dibattito sulle questioni relative all'esatto inquadramento dei sistemi di Intelligenza Artificiale generativa entro la cornice normativa esistente: il tema della riconducibilità all'ambito di tutela della libertà di manifestazione del pensiero dei contenuti prodotti mediante Intelligenza Artificiale generativa. È un dilemma che si intreccia con l'ulteriore nodo, ben più dibattuto in tempi recenti, legato all'estensione ai contenuti prodotti da Intelligenza Artificiale generativa della tutela autoriale.
La domanda potrebbe apparire peregrina e forse mal posta, sol che si pensi che le maggiori preoccupazioni sono emerse, allo stato, rispetto alla produzione di contenuti falsi per supportare campagne disinformative o per danneggiare l'altrui reputazione (con ricorso, per esempio, alla tecnica dei *deepfakes*). Ulteriori dubbi potrebbero manifestarsi ponendo mente al fatto che le costituzioni, come quella italiana all'art. 21, sembrerebbero presupporre che le manifestazioni di pensiero tutelate siano ascrivibili a individui, peraltro esigendone l'identificabilità (l'art. 21 allude, infatti, alle manifestazioni del "proprio pensiero"). Parrebbe così eccentrico domandarsi se le creazioni dell'Intelligenza Artificiale generativa godano di tutela costituzionale come esercizio della libertà di espressione (ponendosi peraltro il problema, in parte analogo all'ambito del diritto d'autore, di discernere tra le ipotesi di utilizzo della tecnica come strumento da parte di persone fisiche "parlanti" e "autori" e quelle di "autonoma" creazione, non servente, dell'Intelligenza Artificiale generativa). La difficoltà di individuare un "parlante" (*speaker*) e di ricollegarvi *free speech rights* potrebbero così risultare argomenti decisivi.
Adottando una diversa prospettiva, tuttavia, si comprende come il tema si sia posto, seppure timidamente, in alcune riflessioni di autori statunitensi. È la prospettiva non del parlante, bensì dell'uditore, del cittadino che ha cioè diritto a informarsi e ricercare con-

tenuti, anche generati dall'Intelligenza Artificiale generativa. Ci si colloca in quello che la giurisprudenza della nostra Corte costituzionale ha indicato come il profilo passivo della libertà di informazione. In questo senso, riorientando la decodificazione del problema, ci si domanda se eventuali limitazioni previste dall'ordinamento alla creazione di contenuti mediante Intelligenza Artificiale generativa risulterebbero rispettose del dettato costituzionale. Il punto è naturalmente molto sentito nell'ordinamento statunitense, dove la libertà di espressione è ancora fermamente modellata sul paradigma del libero mercato delle idee ispirato dalla celeberrima *dissenting opinion* di Justice Holmes del 1919, fedele a una visione pluralistica e diffidente di ogni interferenza di matrice pubblicistica. Proprio il libero fluire e confrontarsi delle idee sarebbe ostacolato da previsioni che, in ipotesi, dovessero prevedere delle limitazioni *content-based,* ossia contenutisticamente sensibili, all'utilizzo dell'Intelligenza Artificiale generativa. Estendere la tutela del Primo emendamento, nella prospettiva del diritto a ricevere informazioni, al prodotto creato artificialmente segnerebbe un limite al potere di contrasto della disinformazione. Al contempo, però, come è stato notato, fungerebbe da salvaguardia rispetto a limitazioni di stampo meno liberale, quali eventuali repressioni del dissenso che i poteri pubblici intendessero perseguire anche nell'utilizzo dell'Intelligenza Artificiale generativa.
Confrontata con l'approccio europeo, questa prospettiva di inquadramento sembrerebbe difficilmente conciliabile con la lotta senza quartiere alla disinformazione che le istituzioni dell'Unione europea hanno inaugurato ormai da tempo. Tuttavia, un "assist" forse involontario nella direzione opposta, di un incontro con la sensibilità statunitense, sembrerebbe potersi cogliere nel disposto dell'art. 28b, par. 4, lett. b), del testo votato dal Parlamento europeo, laddove si prevede che i fornitori di modelli fondazionali utilizzati in sistemi di Intelligenza Artificiale generativa hanno l'obbligo di allenare e sviluppare tali modelli in modo da assicurare tutele adeguate contro la generazione di contenuti in *violazione del diritto dell'Unione europea* e senza pregiudizio ai diritti fondamentali, tra cui la *libertà di espressione* (enfasi aggiunte). Una lettura "in controluce" di questa disposizione, focalizzata sulla natura della disinformazione come contenuto non necessariamente in violazione di legge, sembrerebbe gettare insperatamente un "ponte" tra le sensibilità di Stati Uniti ed Europa.

6. Conclusioni

Le riflessioni esposte senza alcuna pretesa di esaustività rivelano la difficoltà di tracciare uno statuto giuridico adeguato a cogliere e riflettere la complessità intrinseca dell'Intelligenza Artificiale generativa. Difficile da collocare in uno scenario di rischio preciso, sfuggente a norme pensate in tempi recenti per servizi e mercati digitali, di incerta riconducibilità al perimetro di libertà costituzionalmente tutelate, l'Intelligenza Artificiale generativa lancia la sfida ai legislatori delle potenze tecnologiche. Una sfida importante, che si auspica non venga affrontata con l'ansia regolamentare altrove evidenziata da diversi commentatori e senza che la lotta per la sovranità tecnologica finisca per sacrificare diritti e innovazione.

La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica*

Simone Poletti

Abstract

L'elaborato si pone l'obiettivo di analizzare l'innovativo settore della *cybersecurity* e nello specifico il contrasto ai più critici incidenti informatici lesivi della sicurezza nazionale. Il saggio muove dall'analisi delle caratteristiche peculiari e delle contingenze che hanno imposto un cambio di prospettiva nella politica criminale di contrasto a tali condotte criminose, e successivamente indaga la normativa unionale e nazionale con uno specifico *focus* sulla struttura e sui contenuti delle norme istitutive del Perimetro di sicurezza nazionale cibernetica (l. 133/2019) e dell'Agenzia per la cybersicurezza nazionale (l. 109/2021).

The current paper aims to analyse the cybersecurity branch, and in particular the opposition against the most critical cyberattacks concerning national security. This paper begins with the analysis of the peculiarities and the contingencies that have changed policymakers strategies against these criminal behaviours. It then studies the European and national laws with a particular focus on the structures and the contents that establish the national cybersecurity perimeter (l. 133/2019), and those that establish the Cybersecurity national agency (l. 109/2021).

Sommario

Keywords

incidenti informatici – perimetro di sicurezza nazionale cibernetica – resilienza – Direttiva NIS – transnazionalità

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

1. Una prospettiva innovativa: la nascita del Dominio Cibernetico

A partire dallo scorso decennio, all'interno delle grandi potenze economiche mondiali, si è sviluppata una sempre più sentita necessità di concepire la "sicurezza" come un elemento non legato esclusivamente alla sua fisicità e ad una sua estrinsecazione nel mondo esteriore, quanto piuttosto ad un elemento multidimensionale da affrontare in maniera olistica per essere in grado di delineare tutte le sfaccettature in cui essa si concettualizza. Questa innovativa lettura della "sicurezza" ha portato grandi attenzioni alla sua concezione dematerializzata e digitale, generando uno sviluppo esponenziale dell'analisi e degli strumenti per la tutela della sicurezza cibernetica. Ad avvalorare questa affermazione, si consideri il recente riconoscimento da parte della NATO della presenza di un quinto dominio da proteggere (in aggiunta ai quattro domini tradizionali: terreste, marittimo, aereo e spaziale): il dominio cibernetico[1].

La nascita del dominio cibernetico e di conseguenza le istanze di difesa dello stesso, sono determinate dall'utilizzo massivo di strumenti informatici al fine di perpetrare crimini; da una lettura dei rapporti più rilevanti in tema di sicurezza informatica (si pensi ad esempio al rapporto Clusit[2]) è manifesto l'incremento esponenziale dell'utilizzo di dispositivi informatici per finalità illecite. Circa le modalità di esecuzione, bisogna sottolineare la varietà di forme che li caratterizzano (*malware,* sfruttamento di vulnerabilità*, advance persistent threat,* attacchi *DDOS*, ecc.) che sfociano in un utilizzo preponderante di *malware* tendenzialmente di tipo *crypto ransomware*[3]. Un aspetto collaterale che tuttavia riveste un primario interesse per il tema, verte sulle modalità che hanno reso massivo ed esponenziale il fenomeno criminoso, nonostante il numero ristretto di soggetti in possesso delle competenze necessarie per provvedere alla realizzazione dei *software* malevoli. La spiegazione di questa situazione peculiare è rintracciabile nel fenomeno del cd. *malware as a service*[4], da intendersi come vero e proprio mercato digitale – di natura illecita – nel quale un limitato numero di soggetti altamente qualificati nel settore informatico sviluppa *malware* al fine di venderli o porli in locazione a terzi, i quali, seppur inetti con riguardo alle competenze informatiche, sono in grado di reperire ed utilizzare facilmente tali *malware* contribuendo di fatto all'esponenziale crescita degli attacchi informatici.

La nuova centralità della tutela del dominio cibernetico ha portato alla realizzazione di una politica criminale appositamente congegnata per aderire alle particolari caratteristiche degli attacchi informatici, quali la dematerializzazione e l'aterritorialità che

---

[1] A. Marziali, *Cybersecurity: come la NATO si adatta alle nuove sfide | ISPI (ispionline.it),* in *ispionline.it*, 23 giugno 2020.

[2] Si veda *Rapporto Clusit 2022 sulla sicurezza ICT in Italia*, disponibile in clusit.it, marzo 2022, 13 ss.

[3] *Rapporto Clusit 2021 sulla sicurezza ICT in Italia*, disponibile in clusit.it, 2021, 28; E. Kalaimannan - S. John K. - T. DuBose - A. Pinto, *Influences on ransomware's evolution and predictions for the future challenges*, in *Journal of Cyber Security Technology*, 1(1), 2017, 27 ss.

[4] M. Macdonald - R. Frank, *The network structure of malware development, deployment and distribution*, in *Global Crime*, 18(1), 2017, 49 ss.; A.S.A. Bander - M.A. Maarof - S.Z.M. Syed, *Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions,* in *Computers & Security*, 74, 2018, 147-148.

comportano la perdita di rilevanza dei confini nazionali e della spazialità, dal momento che la digitalizzazione permette di operare da remoto a partire da ogni angolo di mondo. La linea di demarcazione che ha portato alla creazione di una politica criminale *ad hoc* focalizzata sul contrasto *ex ante* del fenomeno – mediante l'inserimento di obblighi in capo a soggetti privati, di ingenti sanzioni amministrative pecuniarie e, nel caso italiano, di una fattispecie incriminatrice di pericolo astratto – è determinata dalla severità dell'attacco perpetrato (da valutarsi sulla base del numero di soggetti e dell'area geografica coinvolta, nonché della messa in pericolo per la sicurezza nazionale). Questa tipologia di attacchi, lesiva per l'appunto della sicurezza nazionale, risulta di grande rilievo in quanto è in grado di impedire lo svolgimento di funzioni essenziali o l'erogazione di servizi essenziali, cagionando importanti disservizi sul territorio in grado di ledere diritti costituzionalmente riconosciuti ai cittadini (diritto alla salute, diritto all'istruzione, diritto alla sicurezza ecc.). Proprio la gravità di questo frangente ha spinto alla configurazione ed alla implementazione (sia a livello unionale che a livello nazionale) di misure appositamente congegnate, caratterizzate da elementi *sui generis*; in primo luogo esse si distinguono per la loro spiccata natura preventiva basata sull'assunto per cui il respingimento della totalità degli attacchi informatici risulti impossibile – seppure fortemente implementabile mediante misure di elevato tasso tecnico quali lo sviluppo di strumenti di intelligenza artificiale appositamente predisposti per rilevare nuove tipologie di *malware*[5] – e sul dato incontrovertibile che anche un singolo attacco di severità elevata o critica ai danni di infrastrutture o servizi, in grado pertanto di cagionare una lesione alla sicurezza nazionale, avrebbe conseguenze disastrose; questo motivo ha portato alla creazione di infrastrutture ed architetture cibernetiche congegnate nell'ottica di generare un'elevata sicurezza dei sistemi informatici, al contempo riducendo il numero di attacchi in grado di superare le protezioni ed aumentando la resilienza e la resilienza operativa[6] dei sistemi informatici[7].

Urge sottolineare come questa particolare tipologia di attacchi può rientrare tra le condotte idonee alla configurazione di una cd. *Cyber war* [8], dal momento che nei conflitti contemporanei sempre più spesso a fianco alle condotte tradizionali si pongono azioni altamente digitalizzate ed informatizzate per colpire le infrastrutture critiche – militari e civili – come strategia di indebolimento dell'avversario.

In secondo luogo è fondamentale notare come gli strumenti di contrasto al fenomeno

[5] Si vedano gli interventi di R. Forsi - M. Pereira all'interno del *webinar "*Ransomware, l'intelligenza artificiale a supporto della cybersecurity nella PA e nelle imprese*"*, in cybersecitalia.it, 24 settembre 2021.

[6] Da intendersi come la capacità di un sistema informatico di erogare servizi e rimanere parzialmente in funzione nel momento in cui sta subendo un attacco informatico.

[7] Per un approfondimento sull'importanza del tema della resilienza dei sistemi e del frangente preventivo, si veda l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, Comunicazione congiunta al Parlamento europeo e al Consiglio, *Resilienza, deterrenza e difesa: verso una cybersicurezza forte per l'Ue,* in *ec.europa.eu*, 13 settembre 2017.

[8] Per *Cyber War* si intende un conflitto di natura militare perpetrato in un contesto diverso da quello tradizionale, che si svolge all'interno del dominio cibernetico, con il fine di arrecare danni e malfunzionamenti alle infrastrutture critiche di un Paese mediante l'utilizzo di attacchi informatici. Per un approfondimento sul tema si veda A. Giannulli - A. Curioni, *Cyber war. La guerra prossima ventura,* Fano, 2019.

debbano essere calati in un'ottica unionale ancor prima di quella nazionale in quanto, a causa degli elementi peculiari degli attacchi informatici precedentemente richiamati, la dimensione nazionale e i rigidi confini territoriali nulla hanno a che vedere con queste condotte criminali, caratterizzate da un'elevata flessibilità nell'utilizzo di *server, internet service provider* e reti straniere che permettono di eludere gli strumenti di contrasto operanti in maniera rigida all'interno dei soli confini nazionali.
Un terzo ed ultimo elemento distintivo di tali strumenti è caratterizzato dal ruolo fondamentale che si instaura tra i soggetti pubblici e i soggetti privati, rendendo il partenariato tra essi un perno fondamentale per un efficace ed efficiente funzionamento delle architetture cibernetiche sviluppate[9]. Ciò è determinato dalla rapidità con cui la tecnologia evolve e dalla necessità di ingenti investimenti per mantenere sempre aggiornati gli strumenti e le architetture di contrasto, aspetto che è svolto in maniera più efficiente se ai soggetti governativi viene affiancata un'ampia platea di soggetti privati interessati alla massimizzazione del profitto e all'aggiornamento delle proprie tecnologie.
Questo approccio integrato permette peraltro di incrementare notevolmente l'*awareness* e la *cyber hygene*[10] tra i soggetti privati, elemento di primaria importanza per ridurre l'incidenza e il numero di attacchi informatici con esito positivo.
In termini penalistici tale fenomeno normativo risulta particolarmente interessante dal momento che, con tali previsioni, si è configurato un nuovo paradigma penalistico volto all'anticipazione della tutela penale, necessaria per controbilanciare e rendere maggiormente efficace la politica criminale repressiva contenuta all'interno di fattispecie incriminatrici tradizionali che, seppur ben congegnate, risultano inefficaci a causa delle peculiari caratteristiche che contraddistinguono gli attacchi informatici.

2. La prospettiva sovranazionale

Grazie alla consapevolezza che si è raggiunta sul tema, è stata sviluppata, all'interno dell'Unione europea, un'azione di contrasto armonizzata del fenomeno. Da un punto di vista normativo, l'assetto è variegato sia per la presenza di previsioni nazionali ed unionali, sia per la presenza di diverse tipologie di atti – direttive, regolamenti, comunicazioni ecc. – che generano un'elevata disorganicità sul tema. A livello unionale si possono rilevare due principali misure volte al rafforzamento dei sistemi cibernetici europei: la direttiva (UE) 1148/2016 cd. Direttiva NIS (la quale ha subito un recente aggiornamento) [11] – *Network and Internet Security* – e il regolamento (UE) 881/2019, cd.

[9] L'essenzialità del coinvolgimento dei privati e dei loro investimenti nel settore tecnologico è fortemente richiamata anche dall'ex Direttore dell'ACN Roberto Baldoni. Si veda Palazzo Chigi, *Cybersicurezza, Gabrielli e Baldoni presentano la Strategia nazionale,* in ***youtube.com,*** 25 maggio 2022.

[10] Da intendersi come l'insieme delle buone pratiche che l'utente medio deve praticare nell'utilizzo di dispositivi informatici, al fine di ridurre notevolmente la possibilità di subire un attacco informatico. Per un approfondimento sul tema si veda R. Proli - E. Valguarnera, *Il Cybercrime e le strategie dell'Unione Europea. (dirittopenaleglobalizzazione.it),* in ***dirittopenaleglobalizzazione.it***, 28 agosto 2018.

[11] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, GU 2016 L

Cybersecurity Act [12].

Con la Direttiva NIS si configura, per la prima volta, l'individuazione di alcuni soggetti privati o pubblici – identificati come operatori di servizi essenziali e fornitori di servizi digitali – tenuti a rispettare alcuni obblighi in tema di innalzamento delle misure di sicurezza per i propri sistemi informatici ed in tema di notifica degli incidenti rilevanti subiti. La *ratio* di questa previsione è di garantire una maggior sicurezza dei sistemi e di creare un sistema di comunicazione – strutturato sulla presenza di un punto di contatto unico per ogni Stato membro e sulla presenza di un *cooperation group* a livello unionale per agevolare lo scambio di informazioni – che sia in grado di diffondere le caratteristiche degli incidenti rilevanti subiti al fine di mettere in allerta tutti gli altri operatori rientranti nel perimetro della Direttiva NIS per scongiurare ulteriori attacchi. Seppur il modello e l'ottica di realizzazione sia lodevole, a distanza di più di un lustro è stato possibile notare, oltre a diversi effetti positivi generati, un elenco di difetti che hanno contraddistinto la direttiva; gli aspetti critici sono molteplici, quale l'assenza di un termine specifico entro cui provvedere alla notifica (la quale deve avvenire "senza ritardo"), l'elevata discrezionalità in capo agli Stati membri sia nella individuazione delle autorità competenti sia nella possibilità di comminare sanzioni ai soggetti che non hanno ottemperato alle previsioni della direttiva; tuttavia il difetto più importante riguarda l'eccessiva discrezionalità conferita agli Stati membri nell'identificazione degli operatori di servizi essenziali che ha portato i diversi Stati a procedere "in ordine sparso" utilizzando – a seconda dei casi – un modello granulare o un modello non granulare [13] che ha portato ad una mancata armonizzazione – ravvisata dai *report* del *cooperation group* [14] – aggravata anche dal fatto che le specifiche soglie per l'identificazione degli operatori di servizi essenziali (che riguardano l'impatto dell'incidente, il numero di utenti ed il territorio geografico coinvolti) variano da Stato membro a Stato membro, comportando un inevitabile naufragio della previsione unionale. Queste conclusioni sono possibili grazie alle oculate valutazioni di *assessments* stabilite dalle istituzioni europee, che hanno ottenuto tali riscontri grazie all'apertura di un proficuo dialogo con le società ed i privati europei [15], generando per l'appunto quel partenariato necessa-

194/1*;* direttiva (UE) 2022/2555 del 14 dicembre 2022, del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), GU 2022 L 333/80.

[12] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»), GU 2019 L 171/15.

[13] Per modello granulare bisogna intendere un modello che individua molti differenti sotto-settori all'interno di un macro settore, permettendo una maggior capillarità e specificità nell'individuazione dei soggetti. Il modello non granulare, viceversa, configura l'individuazione di un numero particolarmente ridotto e generico di sotto-settori e in taluni casi si limita all'indicazione di un unico macro settore senza ulteriori specificazioni. Per un'approfondita analisi sul tema si veda *Relazione della Commissione al Parlamento europeo e al Consiglio, di valutazione della coerenza degli approcci adottati dagli stati membri per l'identificazione di servizi conformemente all'articolo 23, paragrafo 1, della direttiva 2016/1148/UE sulla sicurezza delle reti e dei sistemi informativi*, COM (2019), in ec.europa.eu, 28 novembre 2019.

[14] Cooperation Group, *Annual Report NIS Directive Incidents 2019,* in ec.europa.eu, December 2020.

[15] European Commission, *Revision of the Network and Information Security Directive: Questions and Answers*,

rio per uno sviluppo organico e sostenibile degli strumenti di protezione cibernetica. Ciò ha recentemente portato all'accoglimento della proposta di aggiornamento della Direttiva NIS[16], mediante l'emanazione di un atto volto ad ampliare i settori inseriti all'interno della misura ed alla risoluzione delle problematiche sopra indicate[17].

Per quanto invece concerne il cd. *Cybersecurity Act,* l'obiettivo della normativa è parzialmente difforme in quanto il fine ultimo mira alla creazione di un mercato digitale europeo unico caratterizzato da sicurezza ed efficienza per tutti gli operatori e gli utilizzatori[18]. Per garantire ciò, tuttavia, non individua comuni obblighi di implementazione di misure di sicurezza, bensì prevede la creazione di un quadro di certificazione europea per alcuni prodotti *ICT,* consistente in un processo volto alla verificazione della sussistenza dei requisiti minimi previsti dagli *standard* in materia, in grado di verificare la sicurezza cibernetica e l'adeguatezza informatica del bene, con la finalità di garantire l'autenticità, l'idoneità e la sicurezza informatica dello stesso. In tal modo il regolamento mira ad ottenere la *security by design*, cioè la creazione di *software, hardware* ed applicativi europei che siano sicuri ed affidabili fin dalla loro progettazione e non solo in un secondo momento con l'applicazione di idonee misure di sicurezza[19].

Questa previsione, per quanto ad oggi sia rimessa alla mera volontà degli Stati membri, risulta considerevolmente importante anche per il superamento di uno dei maggiori ostacoli che portano le società a non investire in *cybersecurity*, cioè l'incapacità di vedere l'incremento della sicurezza cibernetica dei propri sistemi come un investimento, ma di considerarlo esclusivamente come una spesa da sostenere. Generando un prodotto certificato, autentico e sicuro, riconosciuto come tale a livello unionale, esso ottiene un maggiore valore intrinseco a seguito delle sue comprovate specificità che pertanto pongono le basi per considerarlo un investimento[20].

Per completare il sistema tracciato dal *Cybersecurity Act* bisogna richiamare la fondazione dell'*European Cybersecurity industrial, technology and research competence centre,* cioè il centro di competenza di Bucarest che avrà il compito di mettere in comunicazione il settore pubblico e privato di tutta l'Unione europea per convogliare fondi ed investimenti destinati allo sviluppo della sicurezza cibernetica all'interno dell'Unione[21].

---

in digital-strategy.ec.europa.eu, 19 October 2021; M. Negreiro, European Parliament Research Service, *Briefing – EU Legislation in Progess: The NIS 2 Directive. A high common level of cybersecurity in the EU,* at europarl.europa.eu, December 2021; European Commission, *Commission Staff working document, executive summary of the impact assessment report*, SWD (2020), in eur-lex.europa.eu, 16 December 2020; M. Giuliana Antonio, *Direttiva NIS, la grande riforma: il processo di revisione e i prossimi passi,* in *agendadigitale.eu*, 5 ottobre 2020.

[16] European Commission Proposal, COM/2020/823 final, *Proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive /EU) 2016/1148*, at eur-lex-europa.eu, 16 December 2020.

[17] Direttiva (UE) 2022/2555, cit.

[18] Per una disamina completa sul tema, si veda F. Campara, *Il cybersecurity act,* in A. Contaldo - D. Mula (a cura di), *Cybersecurity Law: disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa, 2020, 57 ss.

[19] R. Proli - E. Valguarnera, *Il Cybercrime e le strategie dell'Unione Europea,* cit.

[20] F. Campara, *Il cybersecurity act,* cit., 57 ss.

[21] Per una panoramica sullo sviluppo della struttura, le competenze ed il funzionamento si veda *cybersecurity-centre.europa.eu.*

3. Le normative nazionali: l'istituzione del Perimetro di Sicurezza Nazionale Cibernetica e dell'Agenzia per la Cybersicurezza Nazionale

Sul piano nazionale l'assetto normativo è peculiare, in quanto il legislatore non si è limitato alla ratifica della Direttiva NIS, bensì ha provveduto alla creazione di uno strumento maggiormente pregnante, quale il Perimetro di Sicurezza Nazionale Cibernetica, mediante l'emanazione del d.l. 105/2019, convertito in l. 133/2019[22].
L'assetto normativo è variegato in quanto oltre alla previsione del decreto convertito in legge, sono stati emanati quattro differenti decreti del Presidente del Consiglio dei Ministri ed un decreto del Presidente della Repubblica; il rimando all'utilizzo di tali previsioni è indicato all'interno della legge sul "Perimetro" che ha rimesso a norme di rango inferiore, da emanare con una cadenzata scansione temporale, una serie di previsioni particolarmente tecniche che difficilmente sarebbero potute essere stabilite in sede parlamentare, garantendo in questo modo una maggior efficienza e celerità nella creazione dell'architettura prestabilita. Urge notare che, per l'emanazione di tali fonti di rango secondario, il legislatore ha saggiamente affiancato al Presidente del Consiglio dei ministri il Comitato Interministeriale per la Sicurezza della Repubblica (CISR), per garantire una maggiore intersettorialità e trasversalità delle previsioni.
Da un punto di vista contenutistico il primo aspetto da sottolineare è la *ratio* della previsione, espressa dall'art. 1, c. 1, che sancisce la garanzia di un'elevata tutela dei sistemi informatici e delle reti che, se interrotti o danneggiati, sono in grado di cagionare un pregiudizio per la sicurezza nazionale [23]. Da questa lettura si può osservare a chiare lettere come la tutela prevista dal "Perimetro" riguardi esclusivamente gli incidenti di particolare gravità in grado di mettere in pericolo lo Stato e la sua sicurezza, risultando estranei alla previsione gli incidenti minori che riguardano la criminalità comune, non in grado di cagionare un pregiudizio sì gravoso. La necessità di provvedere a questa distinzione è quanto mai sentita, dal momento che l'inserimento di un soggetto all'interno del "Perimetro" è tutt'altro che indifferente per tale soggetto, che risulta onerato da alcuni obblighi e limitazioni particolarmente stringenti ed economicamente rilevanti di cui deve farsi carico; per siffatto motivo è sancita l'esclusione da questa previsione di tutti quei soggetti dai quali non possa scaturire una lesione alla sicurezza nazionale in caso di attacco informatico. D'altro lato un'estensione eccessiva di questa previsione, al di fuori del perimetro di tutela della sicurezza nazionale, genererebbe un'eccessiva anticipazione della tutela penale con conseguente torsione del principio di offensività, ed obblighi eccessivamente ingenti a fronte di un pericolo di insufficiente gravità. A conferma di quanto affermato, i requisiti che permettono alle autorità competenti di individuare i soggetti da inserire all'interno del "Perimetro" sono stringenti e riguar-

[22] L. 133/2019, recante "Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica" (G.U. 272 del 20 novembre 2019).

[23] Art. 1, c. 1, l. 133/2019: «[…] assicurare un livello elevato di sicurezza delle reti, dei servizi informativi e dei sistemi informatici […] da cui dipende l'esercizio di una funzione essenziale dello stato, ovvero la prestazione di un servizio essenziale […] dal cui malfunzionamento, interruzione […] ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale».

dano esclusivamente gli operatori che erogano servizi essenziali o svolgono funzioni essenziali, ma che al contempo devono essere dotati di una rete e di sistemi informatici che se interrotta o distrutta sia idonea a cagionare una lesione alla sicurezza nazionale. Una volta individuati dalle autorità competenti, tali soggetti, notificati del loro inserimento all'interno del "Perimetro", debbono provvedere alla comunicazione – entro sei mesi – dell'elenco della componentistica *ICT* e delle proprie reti e sistemi informatici, elenco che dovrà essere aggiornato in caso di modifiche o di nuove acquisizioni; la finalità è di garantire la conoscenza approfondita di tutti i sistemi informatici e delle componentistiche che sono parte del "Perimetro" al fine di valutarne e monitorarne l'affidabilità, a protezione della sicurezza nazionale. Interessante notare come, al fine di garantire una più elevata protezione dei sistemi e solo a determinate condizioni [24], sia conferito in capo al Presidente del Consiglio dei ministri il potere di interrompere un sistema informatico a seguito di una crisi cibernetica, per moderare gli effetti negativi cagionati dall'attacco.

Oltre all'onere sopracitato, i soggetti parte del "Perimetro" sono sottoposti a tre differenti obblighi, i quali devono essere rispettati a pena di subire le sanzioni pecuniarie disposte dall'art. 1, c. 9, della legge sul "Perimetro"[25]; inoltre, in caso di mancata comunicazione o false informazioni ai fini dell'aggiornamento degli elenchi della componentistica rientrante nel "Perimetro", l'art. 1, c. 11, della medesima norma predispone un reato di pericolo astratto [26] – si tratta dell'unica fattispecie incriminatrice penale inserita dalla previsione normativa – che punisce, mediante la reclusione da uno a cinque anni, il soggetto agente che operi con il fine di ostacolare le procedure di verificazione dei requisiti per l'inserimento all'interno del "Perimetro" [27]. Sulla bontà di tale

[24] Le condizioni sono particolarmente stringenti e sono contenute all'interno dell'art. 5, l. 133/2019. Queste consistono nella presenza di una situazione oggettiva di crisi cibernetica o di imminente e grave rischio per la sicurezza nazionale, nella indispensabilità della disattivazione di un sistema o una rete, nella durata minore possibile di tale assenza di fruibilità della rete ed infine del requisito di proporzionalità.

[25] Art. 1, c. 9, l. 133/2019. Nello specifico le singole sanzioni riguardano: «[...] il mancato adempimento degli obblighi di predisposizione e di aggiornamento dell'elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera b); il mancato adempimento dell'obbligo di notifica di cui al comma 3, lettera a); l'inosservanza delle misure di sicurezza di cui al comma 3, lettera b); la mancata comunicazione di cui al comma 6, lettera a), nei termini prescritti; l'impiego di prodotti e servizi sulle reti, sui sistemi informativi e l'espletamento dei servizi informatici di cui al comma 2, lettera b), in violazione delle condizioni imposte dal CVCN o in assenza del superamento dei test di cui al comma 6, lettera a); la mancata collaborazione per l'effettuazione delle attività di test di cui al comma 6, lettera a); il mancato adempimento delle prescrizioni indicate dal Ministero dello sviluppo economico o dalla Presidenza del Consiglio dei ministri in esito alle attività di ispezione e verifica; il mancato rispetto delle prescrizioni di cui al comma 7, lettera b)».

[26] Art. 1, c. 11, l. 133/2019: «Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a cinque anni e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote».

[27] Per una disamina completa sulla fattispecie incriminatrice si rimanda a L. Picotti, M.R. Vadalà, *La nuova legge sulla sicurezza cibernetica (l. 133/19): i profili penalistici | Sistema Penale | SP"*, in *sistemapenale.it,* 5

previsione si pongono alcuni dubbi; se da un lato la struttura della fattispecie come reato di pericolo astratto può essere parzialmente accettata per l'elevata importanza del bene giuridico tutelato, d'altro lato questa decisione presta il fianco alle critiche tradizionali che accompagnano i reati di pericolo astratto circa la torsione del principio di offensività.

Un ulteriore problema, di carattere generale, riguarda il rischio di incrementare una già esasperata proliferazione di fattispecie incriminatrici *extra codicem* generando disorganicità e confusione tra le diverse previsioni. Questo aspetto vale non solamente per la fattispecie incriminatrice bensì anche per le norme settoriali in tema di sicurezza cibernetica che, a seguito della creazione di due previsioni di carattere generale quali le leggi istitutive del "Perimetro" e dell'Agenzia per la Cybersicurezza Nazionale, rischiano di creare sovrapposizioni pericolose di ardua interpretazione. Si auspica un riordino della materia a seguito della definitiva entrata in funzione dell'Agenzia, momento focale per una prima valutazione completa sull'architettura predisposta e sul suo funzionamento.

Conclusa tale parentesi inerente alle sanzioni predisposte, il primo obbligo è previsto dal d.P.C.M. 81/2021[28], in ottemperanza all'art. 1, c. 3, della legge sul "Perimetro", ed impone di apportare ed implementare le idonee misure di sicurezza cibernetica ai propri sistemi; queste misure devono essere predisposte con finalità differenti tra loro in quanto devono essere in grado di aumentare la possibilità di identificazione dei punti deboli della propria architettura cibernetica, incrementare il livello di protezione dei sistemi ed essere in grado di rilevare e rispondere alle eventuali minacce ravvisate, oltre al fatto di garantire un ripristino dei sistemi celere ed adeguato a seguito di un incidente.

Il secondo obbligo – disposto dal medesimo decreto di cui sopra, ai sensi dell'art. 1, c. 2, lett. b) – risulta particolarmente importante ai fini dell'incremento della sicurezza degli operatori, dal momento che prevede la necessità per i soggetti parte del "Perimetro" di notificare celermente allo CSIRT nazionale (*Computer Security Incident Response Team*[29]) l'incidente, allegando le sue caratteristiche; la finalità di questa notifica è duplice: da un lato lo CSIRT nazionale fornisce direttive al soggetto colpito al fine di ripristinare quanto più velocemente possibile e con le modalità idonee i sistemi informatici colpiti, d'altro lato permette allo CSIRT nazionale di comprendere le caratteristiche dell'attacco e le finalità, in modo tale da creare *patch,* aggiornamenti e *best practices* da condividere con tutti gli altri soggetti del "Perimetro" per limitare l'ondata infettiva del *malware* o più in generale dell'attacco perpetrato.

L'aspetto più discusso permane quello legato alle tempistiche, le quali richiedono la notifica entro un'ora nel caso di incidenti gravi (ad esempio *system failure* o danneggiamento di un sistema informatico) e di sei ore per gli incidenti meno gravi (ad esempio

dicembre 2019.

[28] D.P.C.M. 81/2021, recante "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informatici e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n.105, convertito, con modificazioni, dalla legge 18 novembre 2019, n.133, e di misure volte a garantire elevati livelli di sicurezza" (G.U. 138 dell'11 giugno 2021).

[29] Il *Computer Security Incident Response Team* (CSIRT) è l'organismo che si occupa della risposta e del recupero del sistema informatico colpito dall'attacco informatico. Le sue competenze sono di elevata tecnicità ed il suo ruolo risulta centrale nel contrasto agli attacchi cibernetici.

le condotte di infiltrazione e di *lateral movement* all'interno dei sistemi); è stato riscontrato dagli esperti del settore come questo frangente temporale sia eccessivamente limitato per comprendere la tipologia dell'attacco, redigere il rapporto e notificarlo allo CSIRT mentre contestualmente si opera per delimitare e contrastare la minaccia[30]. A render ancor più oneroso l'obbligo, recentemente è stato inserito un ulteriore aggravio alla notifica – per la quale bisogna provvedere entro settantadue ore – per gli incidenti subiti dai soggetti parte del "Perimetro", ai danni di sistemi informatici di loro proprietà ma non facenti parte del "Perimetro"[31]. Questa previsione pare esulare dalla *ratio* di tutela della sicurezza nazionale, seppur finalizzata ad aumentare la sicurezza dei sistemi informatici nazionali. A mero titolo informativo bisogna indicare la presenza della possibilità di provvedere ad una notifica volontaria (di cui all'art. 4 del d.P.C.M. 81/2021), anche per quei casi che non rientrano all'interno del novero di incidenti per i quali la notifica risulta obbligatoria; permangono tuttavia notevoli dubbi circa le modalità, dal momento che la norma risulta silente sul tema.

L'ultimo obbligo – in ottemperanza all'art. 1, c. 6, della legge sul "Perimetro" – è posto in tema di *procurement*, da intendere quale fase di acquisizione di nuova componentistica *hardware* e *software* da parte dei soggetti all'interno del "Perimetro". La finalità è quella garantire una tutela più completa possibile per i sistemi informatici, ponendo dei vincoli di sicurezza ed affidabilità anche ad ogni strumentazione o componente *ICT* che il soggetto abbia intenzione di inserire all'interno dei propri sistemi. Con tale previsione, sancita dal d.P.R. 54/2021[32] e da due ulteriori d.P.C.M.[33], si impone al soggetto parte del "Perimetro" di notificare al Centro di Valutazione e Certificazione Nazionale (CVCN) la volontà dell'acquisizione di nuova componentistica, la quale sarà sottoposta a test specifici sulla sicurezza e sull'affidabilità della stessa, svolti dai Laboratori Applicativi di Prova (LAP) accreditati presso il CVCN. Tale componentistica, pertanto, sarà soggetta alla condizionalità del superamento dei test, senza i quali non potrebbe essere inserita nei sistemi informatici parte del "Perimetro". Se da un lato questa misura è di fondamentale importanza per il mantenimento della sicurezza anche durante gli aggiornamenti delle reti informatiche, dall'altro lato cagiona rallentamenti nella fase acquisitiva – per i test sono previsti infatti quarantacinque giorni di tempo, prorogabili fino a sessanta giorni nei casi eccezionali – e genera ulteriori oneri

[30] S. Mele, *Convegno:* "*Le nuove reti per l'industria italiana e per i consumatori*", 8 aprile 2021, in cybersecitalia.it; M. Santarelli, *Perimetro cibernetico, un'ora per denunciare un incidente: modalità e impatti per le aziende*, in *cybersecurity360.it,* 4 febbraio 2021.

[31] F. Cerciello, *Nuovi obblighi di notifica degli incidenti: quali conseguenze per i soggetti inclusi nel PSNC,* in *cybersecurity360.it*, 29 settembre 2022.

[32] D.P.R. 54/2021, recante "Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133" (G.U. 97 del 23 aprile 2021).

[33] D.P.C.M. 81/2021, recante "Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133" (G.U. 198 del 19 agosto 2021); d.P.C.M. 92/2022, recante "Regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra Centro di Valutazione e Certificazione Nazionale, i laboratori di prova accreditati e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa, ai sensi dell'articolo 1, comma 7, lettera b), del decreto-legge 21 Settembre 2019, n.105, convertito, con modificazioni, dalla legge 18 Novembre 2019, n. 133*"* (G.U. 164 del 15 luglio 2022).

finanziari, incrementando la pressione economica per i soggetti parte del "Perimetro". Sul tema, infatti, la quasi totalità della dottrina si esprime in termini critici circa l'assenza della defiscalizzazione degli investimenti in tema di *cybersecurity*[34] che avrebbe incentivato una crescita tecnologica sostenibile ed ambienti cibernetici maggiormente sicuri.

Risulta interessante notare come ci sia una continuità nelle previsioni nazionali ed unionali, in quanto entrambe perseguono lo stesso obiettivo di un ambiente cibernetico, e quindi di un mercato digitale, che sia sicuro ed efficiente, e ciò viene ricercato mediante la già citata creazione di una *cybersecurity by design*, che permetta un'attenzione alla sicurezza fin dalle fasi progettuali e non esclusivamente come un mero attributo valutato *ex post,* generando maggiore sicurezza e maggior valore intrinseco dei beni in tal modo progettati.

A *latere* di quest'ottica composita e multiforme creata con il "Perimetro", si pone la nascita dell'Agenzia per la Cybersicurezza Nazionale (ACN) con la l. 109/2021. Trattasi di un evento fondamentale per l'incremento della sicurezza cibernetica nazionale; l'Agenzia ha visto la luce a seguito della pressante necessità della creazione di un'*authority* di elevatissima competenza in ambito di sicurezza cibernetica [35]. Precisamente l'Agenzia ha assorbito le competenze che precedentemente erano ripartite tra un elevato numero di soggetti non adeguatamente competenti sul tema, situazione che aveva portato all'inefficacia ed alla disorganicità del sistema; tuttavia sarebbe sbagliato pensare che l'Agenzia racchiuda al suo interno qualsivoglia competenza in ambito di sicurezza cibernetica, in quanto la stessa svolge un ruolo centrale solo per quanto riguarda la sfera dell'incremento e del mantenimento della resilienza dei sistemi informatici nonché il recupero degli stessi in caso di incidente (questo specifico ruolo è svolto dallo CSIRT nazionale in seno all'Agenzia a seguito della trasmigrazione dal DIS)[36].

Tra le competenze che non sono incardinate presso l'Agenzia, per garantire una maggior efficienza del sistema, si annovera l'aspetto repressivo, demandato principalmente alla Polizia di Stato nella sua specialità della Polizia Postale e delle Comunicazione e del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.) soggetto preposto agli interventi nel caso di incidenti rientranti nel "Perimetro", l'attività di *threat intelligence*, demandata alle Agenzie di Intelligence (Agenzia informazioni e sicurezza interna (AISI) ed Agenzia informazioni e sicurezza interna (AISI)) e l'attività di difesa cibernetica militare, demandata al dicastero della

[34] F. Fabbri, *Consiglio Ue su attacchi informatici. Intervista a Stefano Mele*, in *cybersecitalia.it,* 26 febbraio 2021; A. Tofalo, *CyberSec2022. Tofalo (Comm. Difesa): "La sicurezza deve essere un investimento, bisogna defiscalizzare i costi per la cyber"*, ivi, 7 marzo 2022.

[35] Si pensi che si è iniziato a disquisire della necessità di una Agenzia *ad hoc* da diverso tempo; il Comitato parlamentare per la sicurezza della Repubblica (COPASIR), per esempio, ne aveva indicato la necessità nel 2019 e successivamente l'ex sottosegretario di Stato alla Presidenza del Consiglio, autorità delegata per l'informazione e la sicurezza nonché ex capo della Polizia di Stato, Franco Gabrielli, ha espresso la necessità di creare una struttura *ad hoc* per sottrarre al DIS competenze che non gli appartenevano. Si veda, COPASIR, A. Urso, *Relazione sull'attività svolta dal 1° gennaio 2021 al 9 febbraio 2022*, in *parlamento.it;* F. Gabrielli, *Sicurezza. Audizione di Franco Gabrielli alla Camera: creazione di un'Agenzia per la Cybersecurity | Ministero dell'Interno*, in *interno.gov.it*, 30 giugno 2021.

[36] Si veda l'intervento di N. Ciardi presso il Convegno, *Nuove minacce criminali*, Roma, in *cybersecitalia.it,* 3 febbraio 2022.

Difesa e ad un organismo *ad hoc* di recente formazione quale il Comando per le Operazioni in Rete (COR).

Da un punto di vista operativo, l'Agenzia funge da vero e proprio punto di riferimento per i soggetti e le autorità facenti parte ed operanti nel "Perimetro"; grazie alla recente emanazione della strategia di cybersicurezza[37], ha fornito indicazioni sugli obiettivi e sulle modalità di raggiungimento degli stessi in tema di sicurezza e resilienza dei sistemi, e fornisce inoltre – mediante una comunicazione diretta con gli operatori e tramite il suo sito istituzionale e quello dello CSIRT[38] – *best practices*, *alert*, indici di compromissione ed ogni qualsivoglia comunicazione importante per la protezione o per il recupero dei sistemi informatici. In quest'ottica si nota l'importanza dell'obbligo di notifica previsto dalla normativa istitutiva del "Perimetro", in quanto essa garantisce una miglior continuità negli aggiornamenti per affrontare le ultime minacce tecnologiche palesatesi. L'Agenzia risulta fondamentale anche nel ruolo di implementazione del partenariato tra il settore privato ed il settore pubblico, aspetto deducibile dall'osservazione della strategia dalla quale emergono i tre pilastri fondamentali alla base dell'Agenzia: non solo la protezione e la risposta, aspetti precedentemente trattati, ma anche lo sviluppo. Quest'ultimo elemento risulta dirimente, in quanto, in un settore altamente tecnologico come quello della sicurezza cibernetica, sviluppare tecnologie all'avanguardia per rimanere al passo con le minacce risulta essenziale e l'unica modalità per garantire ciò è permettere l'inserimento dell'investimento e delle capacità di ricerca del settore privato[39]. A conferma di ciò, si pensi che l'Agenzia è stata indicata come punto di contatto unico con il Centro per le Competenze Europeo con sede a Bucarest, per garantire uno sviluppo che non sia condizionato dai confini territoriali, per agevolare lo sviluppo europeo di tecnologie avanzate ed implementare il percorso – lungo ed accidentato – che l'Unione europea sta conducendo per il raggiungimento della sovranità tecnologica unionale.

Analizzando la situazione configuratasi, è sempre più evidente la necessaria implementazione di misure e normative che trascendano i confini territoriali nazionali, per procedere – come si stanno adoperando l'Unione europea e i suoi Stati membri – alla creazione di infrastrutture interconnesse tra loro. Ciò è dimostrato anche dalla necessità – sentita fortemente anche dai privati – di aggiornare l'ormai superata Direttiva NIS, con una sua versione che rispecchi effettivamente le necessità degli operatori, cioè di includere un numero più elevato e dettagliato di settori che ad oggi non rientrano in questa *community* di protezione sovranazionale, e di rendere la misura maggiormente armonizzata limitando

[37] Strategia nazionale di cybersicurezza 2022-2026, in acn.gov.it; Palazzo Chigi, *Cybersicurezza, Gabrielli e Baldoni presentano la Strategia nazionale,* cit.

[38] Si vedano acn.gov.it e csirt.gov.it.

[39] L'essenzialità del coinvolgimento dei privati e dei loro investimenti nel settore tecnologico è fortemente richiamata anche dall'ex direttore dell'ACN Roberto Baldoni. Si veda Palazzo Chigi, *Cybersicurezza, Gabrielli e Baldoni presentano la Strategia nazionale,* cit.

Da sottolineare come sia presente uno strumento che mira a favorire questo coinvolgimento tra il settore pubblico e quello privato: in seno all'Agenzia è infatti stato creato uno speciale comitato tecnico scientifico composto da membri della comunità della *cybersecurity* afferenti sia al mondo industriale che al mondo accademico. Per un *focus* sul tema si veda, L. Franchina, *Agenzia cyber, nominato il Comitato tecnico scientifico: quale ruolo nello sviluppo della Strategia cyber nazionale*, in *cybersecurity360.it*, 16 giugno 2022.

la discrezionalità degli Stati membri nella identificazione dei settori e dei soggetti e nella comminazione di sanzioni, onde evitare la creazione di "sacche" di criminalità informatiche che possano approfittare dei disallineamenti all'interno dei differenti Stati membri.
Il percorso intrapreso dalle istituzioni unionali, forte degli *assessments* sul tema della cybersicurezza, sta fortunatamente procedendo spedito; infatti, sul finire dello scorso anno, è stata pubblicata nella Gazzetta Ufficiale dell'Unione europea l'aggiornamento della Direttiva NIS (la cui versione originale è stata contestualmente abrogata)[40] che gli Stati membri sono tenuti a recepire entro un termine di ventuno mesi. Le caratteristiche salienti di questo aggiornamento introducono i correttivi a lungo richiesti dai privati, quali: il considerevole ampliamento dei settori interessati agli obblighi previsti dalla suddetta direttiva, finalizzato a garantir loro un'elevata sicurezza cibernetica (con un'attenzione particolare per la tutela della *supply chain* mediante l'innalzamento delle misure di sicurezza cibernetica anche per le piccole società non facenti parte del "Perimetro"); una minor discrezionalità in capo agli Stati membri per quanto concerne l'identificazione di tali soggetti, grazie all'introduzione di un criterio dimensionale maggiormente organico volto ad armonizzare il novero dei soggetti rientranti nel "Perimetro" e grazie alla rideterminazione dei medesimi attori che vengono ora suddivisi in soggetti essenziali e soggetti importanti; l'introduzione di un termine di ventiquattro ore entro cui provvedere all'inoltro di un preallarme dell'attacco informatico e di un termine di settantadue ore per provvedere alla notifica dettagliata dell'incidente allo CSIRT competente (la direttiva risulta dettagliata sul tema, in quanto enuncia le caratteristiche degli incidenti significativi che sono oggetto dell'obbligo della notifica)[41].
Le novità apportate dall'aggiornamento della direttiva NIS sono puntuali e risultano, al momento, dei correttivi validi, quanto meno sulla carta; bisogna ora attendere gli ulteriori sviluppi osservando il recepimento della direttiva da parte degli Stati membri e i successivi atti unionali volti a fornire maggior dettaglio circa le misure tecnico-operative ed organizzative che saranno imposte ai soggetti parte del "Perimetro" al fine di elevarne la sicurezza cibernetica.
Risulta infine interessante notare come, all'interno delle proposte accolte nell'aggiornamento della Direttiva NIS, si rintraccino molti elementi analoghi o comuni con quelli del Perimetro di Sicurezza Nazionale Cibernetica, ed il fatto che queste proposte siano l'esito di interazioni tra le istituzioni unionali e le società private, dimostra come almeno sulla carta la struttura del "Perimetro" – al netto delle sue criticità che solo con il tempo ed un adeguato rodaggio potranno essere mano a mano depurate – sia una struttura vincente, destinata a portarci verso una maggiore sicurezza cibernetica ed al raggiungimento degli obiettivi rimarcati a più riprese dall'Unione europea: la creazione di un mercato digitale europeo sicuro ed efficiente, ed il raggiungimento della sovranità tecnologica europea.

[40] Direttiva (UE) 2022/2555, cit.

[41] Per una disamina approfondita sulle novità apportate dalla cd. Direttiva NIS 2, si vedano: *Direttiva NIS 2: ecco come prepararsi a recepire i nuovi obiettivi di cyber security*, in *cybersecurity360.it*, 9 gennaio 2023; P. Licata, *Infrastrutture critiche e digitali, in vigore le direttive Nis 2 e Cer (corrierecomunicazioni.it)*, in *corrierecomunicazioni.it,* 16 gennaio 2023; D. Singh Dhoor, *Cibersicurezza, la Direttiva NIS 2 (altalex.com)*, in *altalex.com,* 24 gennaio 2023; G. Zappaterra, *Direttiva NIS2 approvata: i nuovi obblighi di cyber sicurezza per le aziende*, in *agendadigitale.eu,* 15 novembre 2022.

Elenco autori

Marco Bassini
assistant professor of fundamental rights and Artificial Intelligence, Tilburg University
Emanuele Birritteri
assegnista di ricerca in diritto penale, LUISS Guido Carli
Cristiana Carletti
professore associato di diritto internazionale, Università Roma Tre
Alessandro Cupri
dottorando di ricerca in diritto e società plurale, Università degli Studi di Milano-Bicocca
Luca D'Agostino
dottore di ricerca in "Diritto e impresa", docente a contratto, LUISS Guido Carli
Guido d'Ippolito
Funzionario, Autorità garante per la protezione dei dati personali
Giulia Formici
ricercatrice di diritto pubblico comparato, Università degli Studi di Milano
Antonio Gullo
professore ordinario di diritto penale, LUISS Guido Carli
Vincenzo Iaia
assegnista di ricerca, LUISS Guido Carli
Simone Poletti
dottore magistrale in giurisprudenza
Francesco Posteraro
già commissario nell'Autorità per le garanzie nelle comunicazioni; avvocato in Roma
Rossella Sabia
assegnista di ricerca in diritto penale, LUISS Guido Carli
Laura Tadiotto
dottoranda di ricerca, Università degli Studi di Padova
Andrea Tigrino
assegnista di ricerca, Università degli Studi di Trento
Domitilla Vanni
professore associato di diritto privato comparato, Università degli Studi di Palermo
Chiara Vescovi
dottoranda di ricerca, Università degli Studi di Milano-Bicocca
Giulio Vigevani
professore ordinario di diritto costituzionale, Università degli Studi di Milano-Bicocca
Pietro Villaschi
assegnista di ricerca in diritto costituzionale, Università degli Studi di Milano
Silvia Vimercati
assegnista di ricerca in diritto costituzionale, Università degli Studi di Milano-Bicocca
Silvio Roberto Vinceti
assegnista di ricerca, Università degli Studi di Modena e Reggio Emilia
Vincenzo Zeno-Zencovich
professore ordinario di diritto privato comparato, Università Roma Tre

CODICE ETICO

La **Rivista di diritto dei media** intende garantire la qualità dei contributi scientifici ivi pubblicati. A questo scopo, la direzione, il Comitato degli esperti per la valutazione e gli autori devono agire nel rispetto degli standard internazionali editoriali di carattere etico.

Autori: in sede di invio di un contributo, gli autori sono tenuti a fornire ogni informazione richiesta in base alla policy relativa alle submissions. Fornire informazioni fraudolente o dolosamente false o inesatte costituisce un comportamento contrario a etica. Gli autori garantiscono che i contributi costituiscono interamente opere originali, dando adeguatamente conto dei casi in cui il lavoro o i lavori di terzi sia/siano stati utilizzati. Qualsiasi forma di plagio deve ritenersi inaccettabile. Costituisce parimenti una condotta contraria a etica, oltre che una violazione della policy relativa alle submission, l'invio concomitante dello stesso manoscritto ad altre riviste. Eventuali co-autori devono essere al corrente della submission e approvare la versione finale del contributo prima della sua pubblicazione. Le rassegne di dottrina e giurisprudenza devono dare esaustivamente e accuratamente conto dello stato dell'arte.

Direzione: la direzione (ivi compresi direttori e vice-direttori) si impegna a effettuare la selezione dei contributi esclusivamente in base al relativo valore scientifico. I membri della direzione (ivi compresi direttori e vice-direttori) non potranno fare uso di alcuna delle informazioni acquisite per effetto del loro ruolo in assenza di un'esplicita autorizzazione da parte dell'autore o degli autori. La direzione è tenuta ad attivarsi prontamente nel caso qualsiasi questione etica sia portata alla sua attenzione o emerga in relazione a un contributo inviato per la valutazione ovvero pubblicato.

Comitato degli esperti della valutazione: i contributi sottoposti a valutazione costituiscono documentazione a carattere confidenziale per l'intera durata del processo. Le informazioni o idee acquisite confidenzialmente dai valutatori per effetto del processo di revisione non possono pertanto essere utilizzate per conseguire un vantaggio personale. Le valutazioni devono essere effettuate con profondità di analisi, fornendo commenti e suggerimenti che consentano agli autori di migliorare la qualità delle loro ricerche e dei rispettivi contributi. I revisori dovranno astenersi dal prendere in carico la valutazione di contributi relativi ad argomenti o questioni con i quali sono privi di familiarità e dovranno rispettare la tempistica del processo di valutazione. I revisori dovranno informare la direzione ed evitare di procedere alla valutazione nel caso di conflitto di interessi, derivante per esempio dall'esistenza di perduranti rapporti professionali con l'autore o la relativa istituzione accademica di affiliazione.

mediaLAWS

ANNO 2023 - CODICE ISSN 2532-9146