medialaws

Rivista di diritto dei media
3/2024 dicembre

ANNO 2024 - 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
Table of contents

Saggi

Note a sentenza

Cronache

Indice
Table of contents

Essays

Case notes

Comments

Sono stati sottoposti a referaggio anonimo a doppio cieco i saggi di Maria Romana Allegri, Maria Esmeralda Bucalo, Alfonso Contaldo, Elena Falletti - Chiara Gallese, Antonio Manganelli, Stella Romano, Marianna Russo, Giorgio Sichera. Sono altresì stati sottoposti a referaggio anonimo i contributi di Alessia Forte, Edoardo Gatelli, Sara Mastropasqua, Giuseppe Muto e Alessandro Nascimbeni

Saggi

L'ambiguo principio (anche costituzionale?) della trasparenza algoritmica fra tecnologia, diritto e linguaggio*

Maria Romana Allegri

Abstract

Questo scritto tenta, in primo luogo, di circoscrivere il perimetro del concetto di trasparenza algoritmica che, come si vedrà, viene in qualche modo a coincidere con quello di spiegabilità dell'algoritmo. Vengono poi evidenziate le difficoltà della traduzione delle regole tecnologiche dal linguaggio naturale a quello delle macchine e prospettati alcuni esempi di tentativi di definizione di indicatori misurabili di trasparenza algoritmica. Successivamente, il saggio rileva alcune incongruenze in tema di trasparenza algoritmica nella recente *digital regulation* dell'Unione europea (regolamento sulla protezione dei dati, regolamento sui servizi digitali, regolamento sull'intelligenza artificiale). L'utilizzo di algoritmi nel processo decisionale delle pubbliche amministrazioni è stato oggetto di alcune interessanti pronunce del Consiglio di Stato e della Corte di cassazione, non prive tuttavia di incertezze. In conclusione, si formulano alcune osservazioni relative ai principali risultati di questo studio e alla possibilità di considerare la trasparenza algoritmica un principio di rango costituzionale.

This paper attempts, first of all, to circumscribe the perimeter of the concept of algorithmic transparency which, as will be seen, somehow coincides with that of algorithmic explainability. The difficulties of translating technological rules from natural language to that of machines are then highlighted and some examples of attempts to define measurable indicators of algorithmic transparency are presented. Subsequently, this essay underlines some inconsistencies regarding algorithmic transparency in the recent digital regulation of the European Union (data protection regulation, digital services regulation, artificial intelligence regulation). The use of algorithms in the decision-making process of public bodies has been the theme of some interesting rulings from the Council of State and the Court of Cassation, albeit with some uncertainty. In conclusion, some comments are expressed regarding the main results of this work and the possibility of considering algorithmic transparency a principle of constitutional rank.

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

Sommario

Keywords

Intelligenza artificiale – algoritmi – *Machine learning* – trasparenza – pubblica amministrazione

1. Introduzione

I sistemi di intelligenza artificiale, indipendentemente dalle loro varie e non sempre univoche definizioni, stanno diventando rapidamente una parte integrante della nostra vita quotidiana, tanto da poter parlare di "macchine sociali"[1], di "costrutti sociotecnici"[2] o ancora di "istituzioni socio-digitali"[3] in riferimento all'interconnessione di elementi umani e tecnologici. Il recente Regolamento europeo sull'intelligenza artificiale[4] li definisce come sistemi automatizzati progettati per funzionare con diversi livelli di autonomia e adattabilità, che ricevono *input* e generano *output* – quali previsioni, contenuti, raccomandazioni o decisioni – che possono influenzare ambienti fisici o virtuali» (art. 3, c. 1).

L'associazione uomo-macchina – cioè, la stretta interazione fra esseri umani e sistemi informatici – è ormai un elemento strutturale nel nostro ecosistema: gli algoritmi definiscono e limitano l'orizzonte epistemico degli individui, determinando le modalità di connessione fra loro e con il mondo esterno, le opportunità di conoscenza e le possibilità di scelta, fino al punto da interferire con la libertà morale e con la costruzione e rappresentazione dell'identità personale[5]. Ciò è amplificato anche dal fatto che oggi gli elementi in base ai quali le persone compiono le proprie scelte sono sempre più frequentemente forniti da sistemi tecnologici che, attraverso varie forme di *nudging*[6]

[1] A. Simoncini, *Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti*, in *Rivista AIC*, 2, 2023, spec. 4. Si veda anche N. Cristianini – T. Scartamburlo, *On social machines for algorithmic regulation*, in *AI & Society*, 35, 2020, 645 ss.

[2] C. Peroli – C.R. Pereira de Lima, *Democrazia come Value-Sensitive Design: un approccio sociotecnico allo sviluppo delle tecnologie basate su principi democratici*, in R*ivista italiana di informatica e diritto*, 1, 2021, 149 ss..

[3] A. Beckers – G. Teubner, *Three Liability Regimes for Artificial Intelligence*, Oxford, 2021. Si veda anche O.G. Loddo, *L'agire sociale ai tempi dell'intelligenza artificiale. Il concetto di "istituzione sociale-digitale*, in *L'Icocervo*, 1, 2024, 359 ss.

[4] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale.

[5] I. De Vivo*, Il sé allo specchio dell'algoritmo. Libertà epistemica e identità individuale*, in A. Sterpa (a cura di), *L'ordine giuridico dell'algoritmo*, Napoli, 2024, 51 ss., spec. 54.

[6] Il *nudging*, traducibile in italiano come "spinta gentile", consiste nell'attitudine espressa da poteri pubblici e privati a indirizzare il comportamento degli individui mediante pratiche persuasive più o meno esplicite, senza ricorrere a comandi, divieti o incentivi economici. Si tratta di una forma di

più o meno esplicito, possono influenzare o persino determinare i comportamenti individuali e collettivi[7].

Stiamo dunque assistendo a una progressiva perdita di centralità dell'elemento antropologico, data la progressiva delega totale o parziale di funzioni cognitive, fin qui considerate esclusivo appannaggio degli esseri umani, a sistemi tecnologici: la tecnologia non è più solo uno strumento per svolgere più efficientemente alcuni compiti, ma diviene soggetto agente che elabora autonomamente le informazioni e assume decisioni che hanno un impatto nella sfera giuridica individuale[8]. Come è stato efficacemente notato, «siamo organismi informazionali (inforg), reciprocamente connessi e parte di un ambiente informazionale (l'infosfera), che condividiamo con altri agenti informazionali, naturali e artificiali, che processano informazioni in modo logico e autonomo»[9].

Non era mai accaduto finora che la tecnologia acquistasse autonomia rispetto agli esseri umani e diventasse capace di dar forma a un ecosistema in grado di svilupparsi, crescere e modificarsi autonomamente, superando gli umani limiti fisici e cognitivi[10]. Oggi, invece, la tecnologia digitale sta comportando una vera e propria ibridazione tra soggetti e oggetti: da una parte gli oggetti tecnologici divengono sempre più autonomi nelle decisioni e nelle azioni; dall'altra i soggetti umani delegano sempre più decisioni e azioni a tali strumenti, così che l'algoritmo può considerarsi «non tanto strumento neutrale soggetto al nostro arbitrio, ma quanto un portatore autonomo di una credibilità che sconfina, a tratti, in una veridicità di stampo divino»[11]. Ciò comporta il rischio concreto che le decisioni algoritmiche, per il solo fatto di essere prodotte da sistemi tecnologicamente avanzati, che spesso rendono più semplici vari aspetti della vita umana, vengano considerate acriticamente come l'ordine naturale delle cose[12].

Tutto ciò mette in crisi i principi fondamentali del diritto costituzionale, incardinato

"paternalismo debole", che non vincola le scelte individuali ma si limita ad influenzarle, nel presupposto che gli obiettivi verso cui il *nudging* tende non possono che essere condivisi e che il loro mancato raggiungimento dipende essenzialmente da pregiudizi o preconcetti che è opportuno demolire. Tuttavia, posto che la mancanza di costrizioni legale non implica necessariamente l'assenza di interferenze nella sfera di libertà individuale, il *nudging* può essere considerato incompatibile con il disegno costituzionale secondo cui lo Stato ha il compito di assicurare i presupposti per il godimento delle libertà, non quello di orientare le scelte dei singoli. Si vedano in proposito, *ex multis*, Q. Camerlengo, *Costituzione e coscienza sociale: il contributo della teoria del "nudge",* in *Lo Stato*, 21, 2023, 11 ss.; I. Carter*, Il disagio liberale di fronte al nudging*, in *Il Politico*, 1, 2023, 133 ss.; A. Gragnani, *Nudging e libertà costituzionale*, in *Dirittifondamentali.it*, 1, 2021, 498 ss.; M. Miravalle, *Gli orizzonti della teoria del "nudging" sulla normatività: verso un diritto senza sanzioni?*, *in BioLaw Journal*, 1, 2020, 441 ss.; C.R. Sunstein*, Effetto nudge: La politica del paternalismo libertario*, Milano, 2015; R.H. Thaler – C. R Sunstein, *Nudge: The Final Edition*, London, 2021; A. Zito, *La nudge regulation nella teoria giuridica dell'agire amministrativo. Presupposti e limiti del suo utilizzo da parte delle pubbliche amministrazioni*, Napoli, 2021.

[7] A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, *in BioLaw Journal*, 1, 2019, 63 ss., spec. 69-70.

[8] A. Simoncini, *Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti*, cit., 8.

[9] L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017, 106.

[10] A. Sterpa e al., *L'ordine giuridico dell'algoritmo*, cit., 1124.

[11] P. Zellini, *La dittatura del calcolo*, Milano, 2018, 186.

[12] A. Sterpa – I. De Vivo – C. Capasso, *L'ordine giuridico dell'algoritmo: la funzione regolatrice del diritto e la funzione ordinatrice dell'algoritmo*, in *Nuovi Autoritarismi e Democrazie*, 2, 2023, 1120 ss., spec. 1152.

sulla centralità della persona umana e sulla garanzia dei diritti individuali, se non del diritto *tout court*, inteso come tecnica di controllo del comportamento umano, veicolata attraverso enunciati linguistici. Nel campo dell'intelligenza artificiale, infatti, il diritto si confronta con altri sistemi di regolamentazione (in particolare, di matrice tecnologica) talvolta in sinergia e talaltra venendone sopraffatto. Non è escluso allora che, nel tempo, i tradizionali metodi e strumenti giuridici perdano gradualmente efficacia, a meno che il diritto non trovi il modo di affrancarsi da una logica semplicemente reattiva rispetto agli effetti della diffusione dell'IA, riuscendo invece ad anticipare la soluzione dei problemi che possono presentarsi nel prossimo futuro, mostrandosi sensibile alle nuove tendenze e ai nuovi rischi e disponibile all'interazione e all'integrazione con diversi sistemi di regole[13].

È stato efficacemente messo in luce come l'evoluzione del *digital environment* sia uno dei fattori alla base del crescente *judicial activism*, nello sforzo di supplire all'inerzia della politica e del legislatore: «*Political inertia (which is not always forced as sometimes power is delegated to courts with a view to avoiding difficult choices) has fostered judicial imagination within the digital era, along with the resulting use of metaphors and frames to adapt legal systems to the peculiarities of the digital realm*»[14]. Analogamente, è stata evidenziata la progressiva affermazione dei "poteri digitali privati", per contrastare la quale sono state prospettate sostanzialmente due soluzioni: l'applicazione orizzontale dei diritti fondamentali nei confronti dei poteri privati e, contemporaneamente, l'identificazione di nuovi diritti adeguati a contrastare le sfide poste dagli algoritmi[15]. La sfida del cosiddetto "costituzionalismo digitale" è proprio quella di arginare l'affermazione del potere illimitato degli attori privati, attraverso strumenti giuridici di livello nazionale, ma soprattutto sovranazionale[16]. Ci si chiede, allora, se nel complesso degli atti normativi prodotti dall'Unione europea per regolare l'utilizzo di algoritmi e di sistemi di IA non possano essere rintracciati principi di rango costituzionale o para-costituzionale e se fra questi non possa essere annoverato il principio della trasparenza algoritmica.

In qualche modo, gli algoritmi svolgono una funzione regolativa simile a quella del diritto: reagendo al caos delle infinite possibilità, ordinano e razionalizzano una molteplicità di elementi, rendendoli fruibili per la mente umana; dunque, in parole povere, entrambi i sistemi (quello giuridico e quello algoritmico) assumono complessità e producono semplicità, anche se gli algoritmi lo fanno con velocità e capacità di elaborazione enormemente superiori rispetto all'armamentario giuridico[17]. Diversamente dagli algoritmi, però, il diritto è uno strumento ordinamentale flessibile, assiologicamente orientato, che lascia spazio all'innovazione, al discernimento e all'interpretazione, che permette il verificarsi di comportamenti e scelte umane in contrasto con

[13] G. Mobilio*, L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica,* in *BioLaw Journal*, 2, 2020, 401 ss., spec. 404-405.

[14] O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet*, Oxford, 2021, 12-13.

[15] Ivi, 200.

[16] G. De Gregorio, *Digital Costitutionalism in Europe*, Cambridge, 2022.

[17] A. Sterpa e al., *L'ordine giuridico dell'algoritmo: la funzione regolatrice del diritto e la funzione ordinatrice dell'algoritmo*, cit., 1126.

i principi giuridici, che nei sistemi democratici è legittimato dalla volontà popolare[18]. Le regole giuridiche sono formulate in termini generali e astratti in modo da potersi adattare ad una varietà di casi, mantenere efficacia coercitiva nel tempo ed estendersi anche a nuove situazioni non previste al momento della loro originaria produzione. Per questo il diritto è espresso in un linguaggio intrinsecamente malleabile e per qualche verso ambiguo, che può produrre effetti solo ricorrendo all'interpretazione e al giudizio dell'uomo. Invece, le regole tecniche sono formulate in un linguaggio formalizzato e preciso, in base a categorie predefinite e scelte predeterminate[19]. Ora, posto che solo il diritto può far sì che la regolamentazione dei diversi fenomeni sia orientata alla preservazione della dignità e della libertà della persona e del pluralismo sociale, occorre difendere la primazia dell'ordine giuridico, cioè dei valori democratico-liberali del costituzionalismo[20]. Tuttavia, tradurre le regole giuridiche in codice informatico, in modo da consentirne l'applicazione automatica, richiede che esse vengano trascritte nel linguaggio formale delle macchine, cosa che comporta inevitabilmente una riduzione del loro grado di generalità e astrattezza e, conseguentemente, della loro flessibilità e adattabilità[21].

È chiaro che qualsiasi sistema tecnologico deriva originariamente da un'attività creativa umana, che quindi è alla base anche della progettazione delle funzionalità algoritmiche. Tuttavia, le dinamiche attraverso cui gli algoritmi "imparano" dai dati, basate su logiche inferenziali e calcoli statistico-probabilistici, spesso non sono comprensibili per le persone umane, nemmeno per gli stessi programmatori degli algoritmi: non possono essere spiegate prima dell'assunzione della decisione algoritmica né possono essere ricavate a posteriori ripercorrendo in senso contrario la catena dei processi, poiché la maggior parte delle decisioni algoritmiche, a differenza di quelle umane, sono basate sul calcolo delle probabilità e non su procedimenti logico-deduttivi in cui il giudizio è il frutto della ponderazione dei diversi elementi in senso non solo utilitaristico-funzionale, ma anche etico. Dunque, persino la pubblicità di informazioni sulle varie fasi dei processi algoritmici può non essere sufficiente ad assicurarne la trasparenza. Eppure, la questione della trasparenza algoritmica come possibile antidoto alla "tecnocrazia" o "algocrazia"[22] ricorre costantemente nella recente produzione normativa e giurisprudenziale in tema di trattamento dei dati, servizi digitali, decisioni automatizzate e intelligenza artificiale, nella convinzione che le persone debbano essere poste in condizione di comprendere la logica sottostante alle decisioni algoritmiche, per poter tutelare i propri diritti. Occorre però evidenziare l'ambiguità connessa

[18] *Ibid.*

[19] E. M. Lombardi, *Norma e algoritmo: alcune considerazioni sul nuovo ordine tecnologico*, in *Giustizia Civile.com*, 7, 2020, spec. 10.

[20] A. Sterpa e al., *L'ordine giuridico dell'algoritmo: la funzione regolatrice del diritto e la funzione ordinatrice dell'algoritmo* cit., 1128.

[21] E.M. Lombardi, *Norma e algoritmo*, cit., 11.

[22] B. Chomanski, *Legitimacy and automated decisions: the moral limits of algocracy*, in *Ethics and Information Technology*, 3, 2022, 1 ss.; J. Danaher, *The Threat of Algocracy: Reality, Resistance and Accomodation*, in *Philosophy and Technology*, 3, 2016, 245 ss.; P. Marrone, *Democrazia epistemica, epistocrazia, algocrazia: alcuni problemi*, in *Paradigmi*, 2, 2022, 307 ss.; F. Zambonelli, *Algocrazia. Il governo degli algoritmi e dell'intelligenza artificiale*, Trieste, 2023.

al concetto di trasparenza algoritmica e la vaghezza dei relativi standard, dovute alla difficoltà di tradurre i processi algoritmici nel linguaggio comune e all'assenza di parametri precisi per valutare l'adeguatezza delle "spiegazioni".
Nelle pagine che seguono, si cercherà in primo luogo di circoscrivere il perimetro del concetto di trasparenza algoritmica che, come si vedrà, viene in qualche modo a coincidere con quello di spiegabilità dell'algoritmo. Verranno poi evidenziate le difficoltà della traduzione delle regole tecnologiche dal linguaggio naturale a quello delle macchine e verranno prospettati alcuni esempi di tentativi di definizione di indicatori misurabili di trasparenza algoritmica. Successivamente, si rileveranno alcune incongruenze in tema di trasparenza algoritmica nella recente *digital regulation* dell'Unione europea (regolamento sulla protezione dei dati, regolamento sui servizi digitali, regolamento sull'intelligenza artificiale). L'utilizzo di algoritmi nel processo decisionale delle pubbliche amministrazioni è stato oggetto di alcune interessanti pronunce del Consiglio di Stato e della Corte di cassazione, che verranno prese in considerazione, evidenziandone le incertezze. In conclusione, si formuleranno alcune osservazioni relative ai principali risultati di questo studio e alla possibilità di considerare la trasparenza algoritmica un principio di rango costituzionale.

2. Lo sfuggente concetto di trasparenza algoritmica

L'algoritmo è una procedura sistematica che produce risposte a interrogativi o soluzioni a problemi attraverso un numero finito di passaggi[23]; ciò significa che l'algoritmo ha natura procedurale, consistendo in una sequenza di *input*, trasformazione e *output*. Mentre gli algoritmi più semplici, che possiamo definire *rule-based*, si basano su istruzioni predefinite, seguono una logica consequenziale a partire da premesse date e non sono in grado di elaborare nuove informazioni o gestire problemi imprevisti, i più evoluti sistemi di *machine-learning* (MLS) sono invece strutturati per migliorare costantemente in base all'esperienza: possono valutare le correlazioni esistenti fra una moltitudine di variabili e risultati per arrivare a creare modelli predittivi in grado di stimare le probabilità di accadimento di eventi o comportamenti futuri. Tanto i MLS *supervised* – cioè i modelli di apprendimento costruiti sulla base di dati di addestramento etichettati, in cui gli esempi di input sono associati a output noti, in modo che l'algoritmo possa apprendere le relazioni tra *input* e *output*[24] – sia quelli *unsupervised* – cioè i modelli non basati su dati etichettati, ma lasciati liberi di analizzare i dati in modo autonomo per identificare *pattern* e relazioni[25] – sono progettati da creatori umani e, di conseguenza, non sono strumenti tecnologici neutrali, ma riflettono inevitabilmente le preferenze, le priorità e i pregiudizi che appartengono consciamente o inconsciamente ai loro progettisti; per questa loro caratteristica, i MLS posso essere strumenti di propagazione e perpetuazione di *bias* cognitivi, ingiustizie, disuguaglianze e distorsioni[26].

[23] *Algorithm,* in *britannica.com.*

[24] *Cosa è l'apprendimento supervisionato?,* in *ibm.com.*

[25] *Cos'è l'unsupervised learning?*, in *ibm.com.*

[26] N. Kossow – S. Windwehr – M. Jenkins, *Algorithmic Transparency and Accountability*, 2021, in

Ciò considerato, il concetto di trasparenza algoritmica (AT), che può essere definito come «*disclosure of information about algorithms to enable monitoring, checking, criticism, or intervention by interested parties*»[27], è inevitabilmente legato al funzionamento interno dell'algoritmo. Bisogna tuttavia distinguere fra una nozione di AT come "azione" – cioè il fatto di fornire informazioni sull'algoritmo ai suoi utilizzatori o alle terze parti interessate, tenendo presente che il "grado di disvelamento" dipende dall'attitudine dei proprietari o degli sviluppatori dell'algoritmo stesso in termini economici, etici e tecnici – e come "percezione" – ovvero l'impatto delle informazioni concernenti l'algoritmo sui destinatari, che è influenzato dalla metodologia usata nella spiegazione nonché dalle caratteristiche e dalla pregressa esperienza dei destinatari: può esistere, infatti, una discrepanza fra la comprensione reale del funzionamento dell'algoritmo e quella semplicemente percepita, anche se gli studiosi divergono su quali siano i fattori più rilevanti alla base di tale discrepanza[28].

L'intrinseca opacità algoritmica e la crescente affermazione dei sistemi di intelligenza artificiale portano a focalizzare l'attenzione sul concetto di "spiegabilità algortimica" (xAT)[29] come antidoto al *black box problem*[30], cioè al fatto che la realizzazione in concreto della trasparenza algoritmica si rivela estremamente difficoltosa in presenza di sistemi algoritmici di *machine learning* che, come le "scatole nere", non permettono ai programmatori, amministratori o utilizzatori di comprenderne i processi di funzionamento e il peso specifico dei diversi parametri elaborati, tanto da rendere impossibile capire le ragioni che hanno condotto il sistema a produrre un determinato risultato. In altre parole, «*a black box predictor is a data-mining and machine-learning obscure model, whose internals are either unknown to the observer or they are known but uninterpretable by humans*»[31]. Quindi, quando si sostiene che il rispetto del principio di trasparenza «si traduce nella garanzia di tracciabilità dei dati e dei procedimenti

che portano i sistemi intelligenti all'adozione della decisione finale»[32] e che «tutte le informazioni relative al metodo di raccolta dei dati, alla loro classificazione, al tipo di algoritmo impiegato e i risultati ottenuti devono essere completamente documentate, cosicché tutti coloro che vi abbiano diritto o interesse possano comprendere le modalità di impiego dei dati esaminati, seguirne il flusso e verificare che la decisione finale sia stata elaborata e adottata correttamente»[33], bisogna aver ben presente il fatto che la tracciabilità dei dati è ostacolata dalla produzione e dall'utilizzo di dati inferiti (cioè

knowledgehub.transparency.org, 5 febbraio 2021, 5 ss.

27 N. Diakopoulos – M. Koliska, *Algorithmic Transparency in The News Media*, in *Digital Journalism*, 5, 2017, 809 ss., spec. 811.

28 T. Bitzer – M. Wiener – W. A. Cram, *Algorithmic Transparency: Concepts, Antecedents, and Consequences. A Review and Research Framework*, in *Communications of the Association for Information Systems*, 52, 2023, 293 ss., spec. 304-306 e 313-316.

29 La sigla corrisponde a *algorithmic explainability*.

30 T. Bitzer e al., *Algorithmic Transparency*, cit., 297.

31 R. Guidotti e al., *A Survey of Methods for Explaining Black Box Models*, in *ACM Computing Surveys*, 5, 2019, 1 ss., spec. 5.

32 M. Fasan, *I principi costituzionali nella disciplina dell'Intelligenza Artificiale. Nuove prospettive interpretative*, in *DPCE Online*, 1, 2022, 181 ss., spec. 191.

33 *Ibid.*

di dati ottenuti attraverso processi di elaborazione secondaria di dati di partenza) e la comprensibilità dei procedimenti seguiti è impossibile nel caso dei sistemi *black box*.
Se esaminata dal punto di vista della progettazione dell'algoritmo, l'opacità può essere determinata intenzionalmente, allo scopo di prevenire o impedire infiltrazioni abusive nei sistemi o proteggere i diritti di proprietà intellettuale e i segreti industriali, ma può anche essere semplicemente una conseguenza, non voluta ma spesso inevitabile, della complessità tecnologica del sistema[34]. Se considerata, invece, con riguardo ai destinatari delle decisioni algoritmiche o agli utilizzatori dei sistemi algoritmici, l'opacità può essere di tipo relazionale – quando è connessa alle diverse possibilità per diverse categorie di persone di avere accesso alle attività di elaborazione di dati che le riguardano – o di tipo tecnologico, se riferita al livello di comprensibilità del funzionamento del sistema da parte degli esperti che hanno pieno accesso ad esso[35]. Occorre allora avere ben presente quale tipo di opacità caratterizza il sistema considerato e, in relazione ad essa, quale tipo di trasparenza occorrere raggiungere[36]. Nel caso di sistemi che presentano un'opacità di tipo relazionale, occorre realizzare la cosiddetta *exoteric transparency*, in modo da permettere alle persone che interagiscono con essi di ricevere e comprendere le informazioni "significative" rispetto ai loro interessi, acquisendo consapevolezza di quale impatto il sistema algoritmo ha avuto o potrà avere nella loro specifica situazione. La *exoteric transparency* non è legata solo ad aspetti tecnologici, ma dipende in larga misura da fattori comunicativi e dialettici finalizzati a far sì che le informazioni siano opportunamente adeguate alle caratteristiche dei loro destinatari[37] e, pertanto, tende a coincidere con la nozione di spiegabilità. Invece, neutralizzando l'opacità di tipo tecnologico – cioè, permettendo agli esperti di arrivare a conoscere i meccanismi di funzionamento interno del sistema – si ottiene la cosiddetta *esoteric transparency*, che può essere raggiunta tramite soluzioni tecniche (ad esempio, le metodologie di *reverse engineering* o di *transparent box design*)[38], certamente utili per gli "addetti ai lavori", ma non per gli utenti comuni.
È stato giustamente osservato che uno dei fattori che rendono difficile la realizzazione in concreto della xAT è quello linguistico: «Attualmente, durante la fase di *input*, il programmatore deve spiegare in linguaggio naturale semplificato il risultato desiderato, elaborare il progetto utilizzando tale linguaggio e successivamente tradurlo in codice. Durante la fase di *output*, invece, è necessario tradurre il codice generato dalla macchina per ricostruire il processo logico e affrontare questioni di responsabilità e controllo umano *ex post*»[39]. A ciò si aggiunge il fatto che alcune lingue – l'inglese in particolare – si prestano meglio di altre tanto nella programmazione algoritmica quan-

[34] M. Grochowsky – A. Jablonowska – F. Lagioia – G. Sartor, *Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory Premises, in Critical Analisys of Law*, 1, 2021, 43 ss., spec. 48.

[35] *Ibid.*

[36] M. Grochowsky e al., *Algorithmic Transparency and Explainability*, cit., 54.

[37] Ivi, 55-57.

[38] Alcune di queste soluzioni tecniche sono descritte in R. Guidotti e al., *A Survey of Methods*, cit.

[39] G. Caravaggion – M. Orofino, *Lingua e costituzione: l'irrompere dei linguaggi algoritmici*, in *Rivista AIC*, 4, 2023, 155 ss., spec. 181.

to nella traduzione del linguaggio algoritmico in quello naturale. Ne deriva che, poiché i sistemi di IA dispongono di un maggior numero di dati originariamente prodotti in lingua inglese rispetto alle altre lingue e li elaborano ed interpretano tenendo conto prevalentemente dei costrutti logico-sintattici della lingua inglese, possono produrre risultati viziati da *bias* di matrice linguistica.

Analogamente, va evidenziata la scarsa flessibilità del linguaggio algoritmico, che può essere modificato solo tramite processi intenzionali di sviluppo e programmazione, rispetto alle lingue naturali. Infatti, «il linguaggio algoritmico è basato su una struttura logica e sintattica chiusa, fondata sulla matematica, mentre le lingue naturali sono intrinsecamente complesse, ricche di sfumature, ambiguità, contestualizzazioni e contaminazioni […] in grado di esprimere una vasta gamma di concetti complessi e astratti (si pensi alla metafora) che possono essere molto sfidanti da rappresentare con precisione nel linguaggio algoritmico: la comunicazione di emozioni, sentimenti, intuizioni e concetti filosofici richiede una ricchezza e una flessibilità che il linguaggio algoritmico non è in grado, nel suo stato attuale, di fornire. Inoltre, le lingue naturali si evolvono nel tempo, si adattano piuttosto rapidamente ai cambiamenti culturali e si contestualizzano all'interno delle comunità linguistiche. Il linguaggio algoritmico, al contrario, è soggetto a standard e regole specifiche che possono essere modificati solo attraverso processi di sviluppo e aggiornamento»[40].

Nonostante queste oggettive difficoltà, sono stati compiuti alcuni interessanti tentativi di definire alcuni standard di trasparenza algoritmica, intesa soprattutto come spiegabilità (xAT), attraverso i quali si mira a raggiungere un più elevato livello di *fairness* (giustizia, equità, correttezza) nell'utilizzo degli algoritmi. Fra questi, i sette *Principles for Algorithmic Transparency and Accountability*, elaborati nel 2017 dalla *Association for Computing Machinery* (ACM)[41]: si tratta sostanzialmente di obiettivi che gli sviluppatori di algoritmi e gli organismi pubblici e privati che se ne servono dovrebbero tener presente tanto nella progettazione quanto nell'utilizzo dei *software* algoritmici, che però non sono corredati da indicazioni su come questi obiettivi possano essere realizzati in concreto.

Occorre poi menzionare le *Algo Rules*, un elenco di nove principi elaborati e pubblicati nel 2019 dal *think tank* tedesco Bertelsmann Stiftung[42]: anche in questo caso, i prin-

[40] Ivi, 183.

[41] Statement on Algorithmic Transparency and Accountability by ACM U.S. Public Policy Council, approved January 12, 2017 ACM Europe Policy Committee, approved May 25, 2017. Questi principi consistono in: 1) consapevolezza (*awareness*) da parte degli utenti sulle modalità di *data processing* e il livello di automazione delle decisioni; 2) accesso e rimedio (*access* e *redress*), cioè la possibilità di individuare e correggere le decisioni errate); 3) responsabilità (*accountability*) da parte dei produttori e degli sviluppatori dei *software* algoritmici per le conseguenze delle decisioni algoritmiche; 4) spiegazione (*explanation*) della logica dell'algoritmo nel linguaggio umano; 5) consapevolezza della provenienza e dell'attendibilità dei dati su cui l'algoritmo si basa (*data provenance*); 6) verificabilità (*auditability*) dei processi seguiti nello sviluppo e nell'utilizzo degli algoritmi, in modo che possano eventualmente essere sottoposti a revisione; 7) accertamento che i sistemi automatizzati funzionino come previsto (*validation* e *testing*).

[42] Bertelsmann Stiftung (ed.), *Algo.Rules Rules for the Design of Algorithmic Systems*, 7 March 2019. I nove principi consistono in: 1) rafforzamento della competenza degli sviluppatori e degli utilizzatori di sistemi algoritmici relativamente alle loro funzioni tecniche e ai loro effetti potenziali; 2) chiara definizione delle responsabilità associate a ciascun ruolo nella catena di progettazione e utilizzazione algoritmica; 3) chiara definizione *ex ante* e pubblicità delle finalità di ciascun sistema algoritmico, nonché periodiche valutazioni del suo effettivo impatto (*impact assesment*); 4) garanzia della capacità di resistenza del sistema

cipi indicati non sono accompagnati dalla definizione di accorgimenti da utilizzare in pratica per poterli realizzare; in particolare, poi, la regola n. 7 – relativa alla necessità di poter sempre mantenere il controllo umano su ogni fase del processo algoritmico, astenendosi dall'utilizzare i sistemi di *machine learning* la cui complessità lo impedisce di fatto – appare di fatto un po' ingenua, considerando la velocità con cui il progresso tecnologico raggiunge frontiere sempre nuove, inimmaginabili fino a poco tempo prima. Qualche passo in avanti è stato compiuto sempre dalla Bertelsmann Stiftung nel 2020, attraverso l'elaborazione di un documento intitolato *From Principles to Practice. An Interdisciplinary Framework to Operationalise AI Ethics*[43], con il quale si è tentato di pervenire alla definizione di indicatori osservabili, che rendano in qualche modo misurabile il raggiungimento di standard etici (*transparency*, *accountability*, *privacy*, *justice*, *reliability*, *enviromental sustainability*) da rispettare nella progettazione e nell'utilizzo di algoritmi. In riferimento alla questione della trasparenza, ad esempio, il documento contiene alcune domande riguardanti l'origine dei *data set* e l'adeguatezza della *disclosure*[44], mentre altri interrogativi riguardano l'affidabilità dei modelli algoritmici utilizzati[45] oppure l'interpretabilità e comprensibilità dei modelli algoritmici per i *target groups* di destinatari[46]. Va segnalata, da ultimo, l'attività dell'ISO[47], che a luglio 2024 ha predisposto una serie di standard tecnici in materia di trasparenza di sistemi di IA[48], la cui pubblicazione è prevista per novembre 2025.

algoritmico rispetto ad attacchi informatici, accessi non autorizzati e manipolazioni, da comprovare mediante appositi test: 5) *labelling*, cioè possibilità per i destinatari finali di poter chiaramente identificare la matrice algoritmica di determinate decisioni o risultati; 6) pubblicità delle informazioni concernenti l'algoritmo in termini facilmente comprensibili, in modo che i destinatari finali possano capire gli effetti diretti e indiretti del sistema algoritmico; 7) possibilità di mantenere sempre il controllo umano sull'intero processo algoritmico e non utilizzo di sistemi di *machine learning* per i quali il controllo umano sia impossibile; 8) monitoraggio costante sui risultati e sugli effetti prodotti dall'algoritmo e pronto intervento correttivo ove necessario; 9) predisposizione di meccanismi di ricorso contro le decisioni algoritmiche, efficaci e di facile utilizzo.

[43] Bertelsmann Stiftung (ed.), *From principles to practice: How can we make AI ethics measurable?,* 2 April 2020.

[44] *Is the data's origin documented? Is it plausible for each purpose, which data is being used? Are the training data set's characteristics documented and disclosed? Are the corresponding data sheets comprehensive?*

[45] *Has the model in question been tested and used before? Is it possible to inspect the model so far that potential weaknesses can be discovered? Taking into account efficiency and accuracy, has the simplest and most intelligible model been used?*

[46] *Are the modes of interpretability target-group-specific and have been developed with the target groups? Who has access to information about data sets and the algorithm/model used? Is the operating principle comprehensible and interpretable? Are the modes of interpretability in their target-group-specific form intelligible for the target groups? Are the hyperparameters (parameters of learning methods) accessible? Has a mediating authority been established to settle and regulate transparency conflicts?*

[47] L'ISO è un'organizzazione internazionale non governativa indipendente, che raggruppa gli organismi di standardizzazione di 164 paesi del mondo ed elabora standard internazionali che contribuiscono a migliorare la qualità e la sicurezza di beni e servizi e, non da ultimo, a facilitarne lo scambio.

[48] ISO/IEC DIS 12792:2024.

3. Il lessico della trasparenza algoritmica nella *digital regulation* dell'UE: nodi irrisolti

La questione dell'implementazione pratica del principio della trasparenza algoritmica, *mantra* ricorrente nella recente produzione legislativa dell'UE in ambito digitale (a cominciare dal regolamento sulla protezione dei dati personali, per arrivare ai più recenti regolamenti sui servizi digitali e sull'intelligenza artificiale), è un problema non ancora risolto. È evidente, infatti, la tendenza ad una certa vaghezza e indeterminatezza lessicale nel dettato normativo, che nasconde l'incertezza di fondo sull'esatto significato da attribuire al concetto di AT. Tale incertezza, come si vedrà anche nel paragrafo seguente, rende difficile valutare la liceità e la correttezza dei provvedimenti amministrativi basati sull'utilizzo di algoritmi. Preliminarmente, quindi, è utile esaminare nel dettaglio le norme vigenti sulla trasparenza algoritmica, che costituiscono – e, nel caso di quelle relative ai sistemi di IA, costituiranno in futuro – la base sui cui si fonda la giurisprudenza che verrà più avanti considerata.

La trasparenza come principio applicabile al trattamento dei dati personali è menzionata, insieme alla liceità e alla correttezza, nell'art. 5, c. 1, lett. a) del GDPR[49]. Ulteriori riferimenti, soprattutto in relazione alla trasparenza come spiegabilità, si trovano nell'art. 12, c. 1, a proposito delle informazioni sul trattamento dei dati da fornire all'interessato «in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori», nonché negli artt.13 (c. 2, lett. f), 14 (c. 2, lett. g) e 15 (c. 1, lett. h), che attribuiscono all'interessato il diritto di ricevere «informazioni significative sulla logica utilizzata» nel trattamento dei dati. Eppure, come si è visto nei paragrafi precedenti, i modelli algoritmici di tipo *black box* possono produrre risultati viziati da pregiudizi e da errori logici non identificabili e non spiegabili, impedendo inoltre di individuare i soggetti su cui dovrebbe ricadere la responsabilità di risultati distorti o pregiudizievoli. Allora, anche in un'ottica di legittimità dell'azione amministrativa, occorre trovare una modalità di applicazione pratica del principio contenuto nell'art. 14, c. 2, lett. g), del GDPR, relativo al diritto dell'interessato di ottenere, in caso processi decisionali automatizzati, almeno le «informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato»: il dettato normativo, infatti, presuppone la consapevolezza di quali informazioni sono da considerarsi "significative", nonostante finora la ricerca in quest'ambito riferita ai sistemi di IA abbia prodotto risultati frammentari e limitati[50].

Il dibattito sull'esistenza e sulla portata di un diritto alla spiegazione degli algoritmi e sul ruolo che dovrebbe (o potrebbe) spettare agli operatori umani nell'esercizio di questo diritto è stimolato anche da una certa ambiguità nella formulazione dell'art 22 GDPR, che sancisce il diritto a non essere sottoposti a decisioni esclusivamente automatizzate e, comunque, ad essere messi in condizione di poter contestare tale

[49] *General Data Protection Regulation* (regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

[50] J. Lu e al., *Good Explanation for Algorithmic Transparency*, 2019, in *papers.ssrn.com*, 11 novembre 2019.

decisione[51]. Mentre il c. 3 dell'art. 22 assicura all'interessato, nel caso di processi automatizzati, «almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione», i c. 1 e 2 del medesimo articolo sono finalizzati ad evitare che le macchine prendano il sopravvento sulla mente umana, ponendo alcune limitazioni all'utilizzo di algoritmi[52]: l'interessato ha il diritto di non essere a sottoposto a decisioni basate unicamente sul trattamento automatizzato dei dati, salvo che non sia necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento o sia autorizzato dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o si basi sul consenso esplicito dell'interessato.

Occorre però chiarire che l'ambito di applicazione degli artt. 15 e 22 del GDPR è diverso da quello degli artt. 13 e 14: questi ultimi si riferiscono al momento che precede l'inizio delle operazioni di *data processing* (trasparenza *ex ante*), mentre gli art. 15 e 22 alla fase in cui il trattamento è in corso, durante la quale l'interessato potrebbe avere necessità di ricevere ulteriori informazioni, come ad esempio quelle relative ai dati inferiti (generati attraverso l'elaborazione algoritmica) o al funzionamento degli algoritmi utilizzati nel trattamento[53]. Dunque, il diritto dell'interessato di ottenere spiegazioni *ex post* concernenti una decisione algoritmica, che sarebbero invece necessarie per poterla eventualmente contestare, non è previsto da nessuna disposizione del GDPR, ma è relegato solo nel Considerando n. 71, che non è una norma giuridicamente vincolante: in assenza di tali spiegazioni, l'interessato non avrebbe la possibilità di esercitare un controllo sull'utilizzo dell'algoritmo. Nel caso di decisioni algoritmiche assunte da poteri pubblici, ci troveremmo davanti a una versione "modernizzata" e tecnologicamente avanzata di oppressione dei diritti e delle libertà individuali, analoga a quelle di cui è costellata la nostra storia[54].

Dunque, il problema del GDPR consiste proprio nel fatto di non prevedere diritti e obblighi in relazione a un livello minimo di requisiti di spiegabilità delle tecnologie algoritmiche[55]: le disposizioni del GDPR sono focalizzate sui diritti dell'interessato (e sui connessi doveri del titolare del trattamento) e non contengono obblighi di *algorithmic disclosure* nei confronti di terzi interessati o della collettività in generale, che sarebbero invece necessarie per guidare l'azione amministrativa e, più in generale, quella di qualsiasi ente anche privato che assume decisioni algoritmiche. Del resto, il GDPR è un regolamento risalente al 2016, quindi piuttosto datato, se si considera la velocità del progresso delle tecnologie digitali e della loro diffusione.

Più recentemente il regolamento europeo sui servizi digitali (DSA)[56], in vigore dal 17

[51] E. Spiller*, Il diritto di comprendere, il dovere di spiegare. Explainability e intelligenza artificiale costituzionalmente orientata*, in *BioLaw Journal*, 2, 2021, 419 ss., spec. 423.

[52] G. De Minico, *Fundamental Rights, European Digital Regulation and Algorithmic Challenge*, in questa *Rivista*, 1, 2021, 9 ss., spec. 28.

[53] C. Colapietro, *Gli algoritmi tra trasparenza e protezione dei dati personali*, in *Federalismi.it*, 5, 2023, 151 ss., spec.160.

[54] G. De Minico, *Fundamental* Rights, cit., 31.

[55] E. Spiller*, Il diritto di comprendere*, cit., 425.

[56] Regolamento (UE) 2022/2065 del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali, noto come *Digital Services Act* (DSA). Sul regolamento in generale si veda, *ex multis*, M. Orofino, *Il Digital*

febbraio 2024, ha compiuto qualche progresso in termini di requisiti di trasparenza anche nei confronti di autorità pubbliche, revisori esperti indipendenti, ricercatori affiliati a organismi di ricerca, singoli utenti e "pubblico" in generale (in quest'ultimo caso, principalmente nella forma di *transparency reports* da pubblicare *ex post*, come indicato agli artt. 15 e 24). È particolarmente interessante l'art. 27, che postula la trasparenza *ex ante* relativa ai sistemi di raccomandazione, i cui «principali parametri utilizzati», nonché qualunque opzione a disposizione dei destinatari del servizio che consente loro di modificare o influenzare tali parametri principali» devono essere specificati «in un linguaggio chiaro e intellegibile». Non è affatto chiaro, tuttavia, in cosa consistano tali parametri, salvo il fatto che, ai sensi del c. 2, essi devono comprendere, come elementi minimi, i criteri più significativi per determinare le informazioni suggerite al destinatario del servizio e le ragioni per l'importanza relativa dei parametri stessi. Il Considerando n. 70 non fornisce ulteriori elementi interpretativi. Si evince, in ogni caso, il *favor* per la trasparenza *by design*, come elemento costitutivo della progettazione tecnologica.
Un altro elemento importante in termini di *transparency by design* è costituito dal divieto, espresso nell'art. 25 DSA, di *dark patterns*, ovvero di interfacce *online* progettate e realizzate in modo da «ingannare o manipolare i destinatari dei loro servizi o da materialmente falsare o compromettere altrimenti la capacità dei destinatari dei loro servizi di prendere decisioni libere e informate». Si tratta però di una prescrizione da implementare, in concreto, sulla base di orientamenti che la Commissione europea dovrà produrre. Inoltre, dalla lettura del Considerando n. 67 si desume che questo tipo di trasparenza non ha molto a che fare con quella algoritmica, quanto piuttosto con la struttura, la progettazione e le funzionalità delle interfacce, che non devono essere ingannevoli né programmate per indirizzare le scelte individuali (*nudging*).
Infine, secondo l'art. 26 DSA, c. 1, lett. d), le piattaforme digitali che presentano pubblicità nelle loro interfacce devono fornire «informazioni rilevanti direttamente e facilmente accessibili dalla pubblicità relative ai parametri utilizzati per determinare il destinatario al quale viene presentata la pubblicità e, laddove applicabile, alle modalità di modifica di detti parametri». Nemmeno qui viene esplicitata la natura di tali parametri, ma il Considerando n. 68 precisa che i destinatari dei servizi devono ottenere «spiegazioni rilevanti sulla logica seguita» nella presentazione dei messaggi pubblicitari e sui principali criteri di profilazione utilizzati, nonché informazioni su come poter modificare tali criteri. Inoltre, il Considerando n. 69 mette in guardia sui rischi della profilazione (*targeting*) con finalità pubblicitarie, per via dei quali il c. 3 dell'art. 26 vieta di utilizzare per la profilazione le categorie speciali di dati personali di cui all'articolo 9, c. 1, del GDPR.
Sia il GDPR sia il DSA si basano su un approccio *risk-based* all'utilizzo di strumenti tecnologici[57]. Il medesimo approccio è seguito dal recente regolamento europeo sull'intelligenza artificiale (*AI Act*)[58], che si propone di istituire un quadro giuridico unifor-

Service Act tra continuità (solo apparente) e innovazione, in F. Pizzetti (a cura di), *La regolazione europea della società digitale*, Torino, 2024, 83 ss.

[57] E. Longo, *La disciplina del "rischio digitale"* in F. Pizzetti (a cura di), *La regolazione europea*, cit., 53 ss.

[58] Regolamento (UE) 2024/1689 del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale.

me per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale nell'UE, in conformità ai valori dell'Unione, promuovendo la diffusione di un'intelligenza artificiale antropocentrica e affidabile, e garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea (Considerando n. 1 e art. 1)[59]. Dunque, data la necessità di garantire la protezione dei dati personali e i diritti di proprietà intellettuale e industriale, eventuali obblighi di *algorithmic disclosure* previsti *ex lege* dovranno consentire «di sottoporre al requisito della trasparenza non l'intero algoritmo, ma solo le informazioni necessarie per conoscere e comprendere i motivi (quindi il procedimento "logico" utilizzato) sottesi alla decisione stessa»[60]. In aggiunta a ciò, nel caso di sistemi di IA ad alto rischio[61] potranno essere previsti ulteriori obblighi di trasparenza in favore di pubbliche autorità e terze parti indipendenti coinvolte nel processo di valutazione tanto dei rischi quanto della conformità degli strumenti tecnologico ai requisiti previsti dalla normativa[62].

Il Considerando n. 27 dell'AI Act richiama esplicitamente gli Orientamenti etici per un'IA affidabile, elaborati dal Gruppo di esperti ad alto livello sull'intelligenza artificiale (HLEG) istituito dalla Commissione europea nel 2018 e pubblicati nel 2019[63]. In tali orientamenti il Gruppo ha elaborato sette principi etici non vincolanti (intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e *governance* dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità), volti a garantire che l'IA si sviluppi in modo affidabile e antropocentrico. In particolare, il requisito della trasparenza è declinato dal punto di vista della tracciabilità («i set di dati e i processi che determinano la decisione del sistema di IA, compresi quelli di raccolta ed etichettatura dei dati, come pure gli algoritmi utilizzati, dovrebbero essere documentati secondo i migliori standard»), della spiegabilità[64] e

[59] Sul regolamento in generale, *ex multis*: C. Casonato – B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, *in BioLaw Journal*, 3, 2021, 415 ss.

[60] C. Colapietro, *Gli algoritmi*, cit., 172.

[61] Gli artt. da 6 a 49 del regolamento, contenuti nel Capo III, si riferiscono ai sistemi di AI ad altro rischio, cioè quelli elencati nell'Allegato III, che ai sensi dell'art. 6 presentano rischi significativi di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di influenzare i processi decisionali; sono sempre considerati ad alto rischio i sistemi che comportano la profilazione delle persone. Ai sensi dell'art. 7, spetta alla Commissione europea il compito di modificare e integrare progressivamente l'Allegato III. Invece, gli artt. 50-56, contenuti nel capo IV e nel Capo V del regolamento, si riferiscono a sistemi di AI diversi da quelli ad altro rischio, ma comunque non privi di un certo livello di rischio.

[62] A tale proposito, il Considerando n. 68 prevede che «ai fini dello sviluppo e della valutazione di sistemi di IA ad alto rischio, è opportuno concedere ad alcuni soggetti, come fornitori, organismi notificati e altre entità pertinenti, quali i poli europei dell'innovazione digitale, gli impianti di prova e sperimentazione e i ricercatori, l'accesso a set di dati di elevata qualità e la possibilità di utilizzarli nell'ambito dei settori di attività di tali attori soggetti al presente regolamento».

[63] Orientamenti etici per un'IA affidabile.

[64] Secondo il par. 77 del documento (a p. 20), «la spiegabilità attiene alla capacità di spiegare sia i processi tecnici di un sistema di IA che le relative decisioni umane (ad esempio i settori di applicazione di un sistema di IA). Affinché un sistema di IA possa essere tecnicamente spiegabile gli esseri umani devono poter capire e tenere traccia delle decisioni prese dal sistema stesso. Potrebbe inoltre essere necessario trovare un compromesso tra il miglioramento della spiegabilità di un sistema (sacrificando la precisione) e l'aumento della precisione (a scapito della spiegabilità). Se un sistema di IA influisce

della comunicazione (i sistemi di IA devono essere identificabili come tali, deve essere preferita l'interazione umana a quella con il sistema e devono essere comunicate agli operatori del settore dell'IA o agli utenti finali le capacità e le limitazioni del sistema). Tuttavia, soprattutto in relazione al requisito della spiegabilità, non è affatto chiaro in che modo i processi tecnologici debbano e possano essere spiegati in modo che siano comprensibili per i destinatari delle decisioni e soprattutto in base a quali parametri si possa valutare l'adeguatezza della spiegazione fornita agli standard richiesti. Questo, come si è più volte evidenziato, rende difficile valutare la legittimità dell'azione amministrativa in caso di utilizzo di IA. Eppure, soprattutto nel caso di sistemi di AI ad alto rischio, i Considerando n. 71 e 72 evidenziano che disporre di informazioni comprensibili sulle modalità di e di funzionamento di tali sistemi è essenziale per consentirne la tracciabilità, verificarne la conformità ai requisiti normativi e svolgere il monitoraggio successivo all'immissione sul mercato. Quindi, i sistemi di IA ad alto rischio dovrebbero essere accompagnati da informazioni adeguate sotto forma di istruzioni per l'uso rivolte ai *deployer*[65] – soggetti privati, ma oggi spesso anche pubblici – concernenti le caratteristiche, le capacità e i limiti delle prestazioni del sistema, i rischi possibili e le pertinenti misure di sorveglianza umana, anche attraverso esempi illustrativi. Per questo «i fornitori dovrebbero garantire che tutta la documentazione, comprese le istruzioni per l'uso, contenga informazioni significative, complete, accessibili e comprensibili, tenendo conto delle esigenze e delle conoscenze prevedibili dei *deployer* destinatari. Le istruzioni per l'uso dovrebbero essere messe a disposizione in una lingua che possa essere compresa facilmente dai *deployer* destinatari, secondo quanto stabilito dallo Stato membro interessato». Ora, a prescindere dal fatto che i Considerando non hanno efficacia normativa, ma solo valore interpretativo, nemmeno la loro verbosità chiarisce adeguatamente in che modo sia in concreto possibile descrivere e spiegare parametri tecnici nel linguaggio naturale, quale livello di chiarezza e precisione nella spiegazione sia necessario e come sia possibile valutarne il raggiungimento.

Venendo al dettato normativo dell'AI Act, l'art. 11 prevede che i sistemi di intelligenza artificiale ad alto rischio debbano essere corredati di una documentazione tecnica da fornire alle autorità nazionali competenti e agli organismi notificati, che deve contenere almeno gli elementi che figurano nell'Allegato IV al regolamento stesso. Si tratta di informazioni, però, non destinate ai *deployer* o agli utilizzatori finali di tali sistemi, ma agli organi nazionali di regolamentazione e controllo. Effettivamente l'Allegato IV è piuttosto preciso e specifico e include, fra le varie informazioni da fornire, anche una descrizione dettagliata degli elementi del sistema di IA e del processo relativo al suo sviluppo, della quale vengono puntualmente indicati i vari aspetti. Permane tuttavia la

considerevolmente sulla vita delle persone, dovrebbe sempre essere possibile richiedere una spiegazione adeguata del processo decisionale del sistema. Tale spiegazione dovrebbe essere tempestiva e adeguata alle competenze del portatore di interesse in questione (un non esperto, un'autorità di regolamentazione o un ricercatore). Dovrebbero inoltre essere disponibili indicazioni sul grado in cui un sistema di IA influenza e plasma il processo decisionale organizzativo, sulle scelte progettuali del sistema e sulla logica alla base della sua distribuzione (garantendo così la trasparenza del modello di business)».

[65] Secondo l'art. 3, c. 4, questo termine, per il quale non è stata prevista una traduzione in lingua italiana, si riferisce a «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale».

perplessità sull'effettiva possibilità di tradurre in modo efficace e davvero comprensibile le regole tecniche dal linguaggio computazionale al linguaggio naturale, in modo da renderle comprensibili a persone non necessariamente esperte del linguaggio matematico-informatico.

Per quanto riguarda, invece, l'utilizzo di sistemi algoritmici da parte di pubbliche amministrazioni, rileva particolarmente l'art. 13, concernente le istruzioni per l'uso rivolte ai *deployer*; queste ultime devono contenere «informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili», concernenti vari aspetti del sistema di AI, fra cui: «il livello di accuratezza che ci si può attendere, comprese le metriche, di robustezza e cibersicurezza»; «le capacità e caratteristiche tecniche del sistema di IA ad alto rischio connesse alla fornitura di informazioni pertinenti per spiegarne l'output»; «le specifiche per i dati di input o qualsiasi altra informazione pertinente in termini di set di dati di addestramento, convalida e prova»; «informazioni che consentano ai *deployer* di interpretare l'output del sistema di IA ad alto rischio e di usarlo in modo opportuno»; «una descrizione dei meccanismi inclusi nel sistema di IA ad alto rischio che consente ai *deployer* di raccogliere, conservare e interpretare correttamente i *log*». Effettivamente, questo elenco di informazioni che devono essere contenute nelle istruzioni per l'uso rappresenta il risultato più avanzato raggiunto finora nello sforzo di dotare il principio di trasparenza algoritmica di indicazioni operative quanto più possibili esaurienti e puntuali. Tuttavia, a parte il fatto che questo "decalogo" si riferisce solo i sistemi di IA considerati ad alto rischio e non a qualsiasi sistema di IA, non si può non evidenziare una certa difficoltà di comprensione di almeno alcune fra varie specifiche richieste nonché, come già sottolineato più volte, una certa ambiguità di fondo: quale livello di accuratezza e precisione è richiesto nelle spiegazioni affinché esse possano essere davvero considerate pienamente comprensibili per i loro destinatari?

Peraltro, è davvero necessario che i *deployer* – e particolarmente i soggetti pubblici che rivestono questo ruolo – acquisiscano un elevato livello di conoscenza del funzionamento del sistema di IA ad alto rischio, visto che l'art. 86, c. 1, attribuisce loro una sorta di ruolo di "mediatori" fra i progettisti e i proprietari dei sistemi algoritmici e i destinatari finali delle decisioni. Questi ultimi, infatti, hanno diritto di ricevere proprio dai *deployer* «spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata», qualora tale decisione abbia un impatto negativo sulla loro salute e sicurezza o sull'esercizio dei loro diritti fondamentali. Anche qui, però, non è affatto chiaro quale livello di dettaglio e di "tecnicismo" debbano avere queste informazioni trasmesse dai *deployer* ai destinatari finali. Comunque, l'art. 96 del regolamento attribuisce alla Commissione europea il compito di elaborare, senza però stabilire alcuna scadenza, orientamenti sull'attuazione pratica delle disposizioni del regolamento.

Le perplessità fin qui espresse assumono particolare rilievo nel caso dei sistemi di IA destinati a interagire direttamente con le persone fisiche (art. 50, c. 1), i sistemi per finalità generali che generano contenuti testuali o audiovisivi (art. 50, c. 2), i sistemi di riconoscimento delle emozioni o di categorizzazione biometrica (art. 50, c. 3) e quelli che generano *deep fakes* manipolando contenuti testuali o audiovisivi (art. 50, c. 4). Si tratta di sistemi non sempre e non necessariamente qualificabili ad alto rischio, ma che pos-

sono esserlo, per lo meno nel caso dei sistemi di identificazione e categorizzazione biometrica e quelli di riconoscimento delle emozioni, elencati nel par. 1 dell'Allegato III. Il Considerando n. 29 è particolarmente esauriente nel presentare tutti i possibili rischi derivanti dalle tecniche di manipolazione basate sull'IA, che «possono essere utilizzate per persuadere le persone ad adottare comportamenti indesiderati o per indurle con l'inganno a prendere decisioni in modo da sovvertirne e pregiudicarne l'autonomia, il processo decisionale e la libera scelta»; ciò è particolarmente vero nel caso di sistemi di IA che impiegano componenti subliminali, che vanno al di là della percezione umana, oppure nel caso delle interfacce *brain-computer* o ancora in quello della realtà virtuale. Occorrerebbe quindi vietare l'utilizzo di questi sistemi nei casi in cui possano verosimilmente provocare danni significativi alle persone. Analogamente, il Considerando n. 44 esprime preoccupazione per i sistemi di IA volti a identificare o inferire emozioni o intenzioni a partire da dati biometrici, non solo per via della loro scarsa attendibilità, ma anche perché potrebbero essere causa di trattamenti discriminatori.

Eppure, nonostante la prolissità dei Considerando, l'art. 50 si limita a prevedere che occorre informare le persone fisiche del fatto che stanno interagendo con un sistema di IA, «a meno che ciò non risulti evidente dal punto di vista di una persona fisica ragionevolmente informata, attenta e avveduta, tenendo conto delle circostanze e del contesto di utilizzo»; inoltre, nel caso di IA generativa, occorre far sì che gli *output* dei sistemi siano marcati in un formato leggibile meccanicamente e rilevabili come generati o manipolati artificialmente, soprattutto nel caso di produzione di *deepfakes*; infine, nel caso di sistemi di riconoscimento delle emozioni o di categorizzazione biometrica, occorre che le persone fisiche che vi sono esposte vengano informate in merito al loro funzionamento. Tutte queste informazioni devono essere «fornite alle persone fisiche interessate in maniera chiara e distinguibile al più tardi al momento della prima interazione o esposizione» (art. 50, c. 5).

Colpisce davvero la stringatezza del dettato normativo, concentrato sul generico obbligo di fornire informazioni, in confronto alla complessità dei possibili rischi evidenziati nei Considerando, senza considerare l'indeterminatezza del parametro relativo al punto di vista della persona ragionevolmente informata e avveduta e di quello relativo alla chiarezza e comprensibilità delle informazioni. Ci si chiede se le caratteristiche delle informazioni da fornire agli utenti di questi sistemi di IA particolarmente rischiosi debbano essere analoghe a quelle che l'Allegato IV e l'art. 13 del regolamento del regolamento hanno previsto rispettivamente per le autorità competenti e per i *deployer* oppure se debbano essere diverse, considerando che dovranno rivolgersi a persone comuni, probabilmente prive di conoscenze specifiche. In ogni caso, il regolamento sui sistemi di IA non lo specifica e tale omissione rappresenta certamente un *vulnus* in relazione alla garanzia dei diritti e delle libertà fondamentali degli individui.

Gli articoli da 51 a 56 del regolamento sulla AI riguardano i modelli di IA per finalità generali[66], definiti dall'art. 3, c. 63, come «un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con

[66] I. Trigueiro e al., *General Purpose Artificial Intelligence Systems (GPAIS): Properties, definition, taxonomy, societal implications and responsible governance*, *in Information Fusion*, 103, 2024, 1 ss.

competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato». Questi modelli – che tendenzialmente non sono inclusi fra quelli ad alto rischio, ma che talvolta possono comportare rischi sistemici nei casi di elevata capacità di impatto, secondo i criteri indicati nell'Allegato XIII – devono essere corredati da una documentazione tecnica (secondo le specifiche indicate nell'Allegato XI) e da informazioni sulla trasparenza, menzionate nell'art. 53, par. 1, lett. b e meglio specificate nell'Allegato XII. Vale anche in questo caso tutto ciò che è stato già scritto sopra a proposito dei requisiti indicati nell'Allegato IV: da un lato, si apprezza lo sforzo di declinare il principio della trasparenza algoritmica in termini pratico-operativi; dall'altro, però, non si può fare a meno di evidenziare l'ambiguità di alcune espressioni che figurano nell'Allegato.

Non va sottaciuto, infine, che l'art. 14 del regolamento sulla IA prevede il principio di sorveglianza umana per tutti i sistemi di IA ad altro rischio (*human in the loop* o HITL)[67], rinforzando così quanto già previsto dall'art 22, c. 3, del GDPR. Ciò significa che il sorvegliante umano – nel caso di sistemi di IA utilizzata dalle PA, un funzionario amministrativo o un tecnico esterno? – deve «comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese», nonché essere capace di «interpretare correttamente l'output del sistema di IA ad alto rischio», in modo da poter decidere di non utilizzare il sistema, intervenire sul suo funzionamento, modificarne il risultato o anche disattivarlo. Ora, a parte il fatto che appare piuttosto ingenuo immaginare che una persona fisica possa avere in ogni momento il pieno controllo di processi algoritmici prodotti da sistemi dotati di capacità di archiviazione, ricerca, elaborazione e calcolo infinitamente superiori a quelle umane, fino al punto da poter interferire con il funzionamento della macchina, è evidente che i descritti compiti di sorveglianza presuppongono a monte la piena realizzazione della xAT a beneficio del supervisore: ma che tipo di informazioni dovrebbero essere fornite a quest'ultimo per porlo in condizione di svolgere efficacemente i propri compiti?[68]

Da ultimo, va evidenziato che il recente regolamento europeo sull'intelligenza artificiale non distingue fra enti pubblici e privati, ma solo fra fornitori e utilizzatori (*deployers*) di sistemi di intelligenza artificiale, senza tenere conto del fatto che, invece, gli enti pubblici dovrebbero essere tenuti a garantire un livello di trasparenza algoritmica tendenzialmente più elevato di quello richiesto ai privati, ai fini della sindacabilità del provvedimento amministrativo[69]. In particolare, la normativa di livello unionale non obbliga i soggetti pubblici che utilizzano algoritmi decisionali a dare pubblicità a questa

[67] B. Marchetti, *La garanzia dello human in the loop alla prova della decisione amministrativa algoritmica*, in *BioLaw Journal*, 2, 2021, 367 ss.

[68] Inoltre, nel caso in cui sia la pubblica amministrazione a servirsi di sistemi algoritmici, ci si chiede se il compito di sorveglianza debba essere svolto da un funzionario amministrativo – che potrebbe non avere adeguate competenze tecniche – o da uno sviluppatore del sistema, che però sarebbe estraneo alla pubblica amministrazione (B. Marchetti, *La garanzia* …, cit., 377).

[69] A. Papa, *Intelligenza artificiale*, cit., 110.

scelta[70], a meno che – come prescrive il GDPR – il sistema non preveda il trattamento di dati personali e quindi sia d'obbligo informare gli interessati delle modalità e finalità del *data processing*. Sarebbe invece utile vincolare per legge le pubbliche amministrazioni a dare pubblicità al fatto di utilizzare algoritmi per lo svolgimento di talune attività rientranti nei loro compiti, anche se a quel punto ci si troverebbe davanti all'ostacolo di come poter assicurare un efficace livello di spiegabilità algoritmica.

In conclusione, da questa rassegna della recente produzione normativa dell'UE sulla trasparenza algoritmica emerge una certa sudditanza delle regole giuridiche nei confronti di quelle tecniche[71]. Dovrebbe invece avvenire il contrario: la norma giuridica dovrebbe precedere – e non seguire faticosamente – le specifiche tecniche dei sistemi, dettando le linee guida per la loro disciplina. Ora, è pur vero che una tecnica normativa che prevede ampio ricorso a concetti indeterminati e interpretabili implica una certa flessibilità applicativa, che potrebbe favorire l'adattamento ai rapidi sviluppi tecnologici, oltre a lasciare spazio alla regolamentazione ad opera delle diverse autorità nazionali competenti; tuttavia, «in mancanza di pratiche applicative comuni, il rischio è che tale indeterminatezza generi anche incertezza, aprendo la possibilità di applicazioni difformi della disciplina all'interno del territorio dell'Unione e un conseguente aumento del contenzioso giudiziario»[72].

---

[70] Ivi, 112.

[71] In effetti, gli articoli contenuti nella quinta sezione del regolamento UE n. 1689/2024 sui sistemi di IA richiamano il precedente regolamento UE n. 1025/2012 sulla normazione europea, modificato dal regolamento n. 2022/2480 del 14 dicembre 2022. Secondo questi regolamenti le cosiddette "norme armonizzate" (trad. it. di *harmonized standards*) – cioè le specifiche tecniche emanate da organismi di normazione internazionali (ISO, IEC), nazionali (per l'Italia, UNI e CEI), ma soprattutto europei (CEN, CENELEC o ETSI), su richiesta della Commissione europea, in base ad orientamenti generali elaborati da quest'ultima – stabiliscono i requisiti essenziali per l'immissione sul mercato europeo di determinati prodotti, volti soprattutto alla protezione della salute e della sicurezza dei consumatori, e quindi rappresentano un elemento chiave per garantire la libera circolazione dei prodotti all'interno del mercato dell'Unione europea. Si tratta di un sistema di partenariato pubblico-privato nel quale, sotto la guida della Commissione europea, organismi tecnici di natura privata elaborano standard tecnici che conferiscono ai produttori la presunzione di conformità ai requisiti della legislazione. L'adozione delle norme armonizzate non è obbligatoria per le imprese; tuttavia, i prodotti che le rispettano mostrano di possedere un determinato livello di qualità, sicurezza e affidabilità e si presumono conformi alla legislazione armonizzata dell'Unione europea, così che, in caso di controversie, l'onere di provare la mancata conformità del prodotto ricade sull'autorità competente e non sull'impresa. I regolamenti UE sulla normazione richiedono, inoltre, che le autorità pubbliche si adeguino a tutte le specifiche tecniche pertinenti per l'acquisto di hardware, software e servizi di tecnologia dell'informazione. Dunque, poiché anche i sistemi di IA sono prodotti commerciali, il regolamento UE sull'IA (quinta sezione) presuppone, salvo prova contraria, che i sistemi di IA ad alto rischio o i modelli di IA per finalità generali conformi alle norme armonizzate – che gli organismi europei di normazione dovranno produrre su mandato della Commissione europea – siano conformi al regolamento. Si veda in proposito, per approfondimento, C. Marenghi, *La proposta di Regolamento UE sull'intelligenza artificiale e la regolazione privata: spunti critici in tema di norme tecniche armonizzate*, in *Diritto comunitario e degli scambi internazionali,* 3-4, 2021, 563 ss.

[72] C. Casonato-B. Marchetti, *Prime osservazioni*, cit., 422-423.

4. L'utilizzo di algoritmi da parte delle pubbliche amministrazioni: qualche indicazione giurisprudenziale e molte incertezze

La giurisprudenza italiana in anni recenti ha affrontato la questione della trasparenza algoritmica, cercando di definire – per la verità senza giungere a risultati soddisfacenti – quale livello di comprensibilità del funzionamento dell'algoritmo sia da considerarsi adeguato. Le sentenze qui esaminate[73] riguardano l'utilizzo di tecnologie algoritmiche nei processi decisionali delle pubbliche amministrazioni che, come è noto, sono tenute ad assicurare l'imparzialità loro agire (art. 97, c. 2, Cost.), nonché la trasparenza «intesa come accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche» (art. 1, c. 1, d.lgs. 33/2013). A scanso di equivoci, va precisato che i casi qui di seguito prospettati si concentrano sulla nozione giurisprudenziale di algoritmo – che lo stesso Consiglio di Stato (sez. III, 25 novembre 2021, n. 7891) ha definito «una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato» – e non di intelligenza artificiale, che, secondo la medesima pronuncia del Consiglio di Stato, comporta una situazione in cui «l'algoritmo contempla meccanismi di *machine learning* e crea un sistema che non si limita solo ad applicare le regole *software* e i parametri preimpostati (come fa invece l'algoritmo "tradizionale") ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico»[74]. Il problema, però, è che fra le due categorie – algoritmo e intelligenza artificiale – non vi è una dicotomia, ma piuttosto una osmosi, posto che i sistemi di intelligenza artificiale funzionano grazie agli algoritmi e che gli algoritmi possono avere complessità variabile, rendendo praticamente impossibile una netta distinzione fra quelli che la sentenza in esame definisce "tradizionali" e quelli basati, invece, sul *machine learning*.

Proprio in considerazione dei diversi livelli di complessità algoritmica, occorre chiedersi, in primo luogo, se la tanto invocata trasparenza possa realizzarsi attraverso l'ostensione del codice-sorgente dell'algoritmo[75], che potrebbe eventualmente essere re-

[73] A. Corrado, *La trasparenza necessaria per infondere fiducia in una amministrazione algoritmica e antropocentrica*, in *Federalismi.it*, 5, 2023, 175 ss.; L. Grimaldi, *Costituzionalismo "post-umano" alla prova della decisione pubblica algoritmica*, in *Federalismi.it*, 34, 2022, 75 ss.; G. Lo Sapio, *La trasparenza sul banco di prova dei modelli algoritmici*, *in Federalismi.it*, 11, 2021, 239 ss.; P. Otranto, *Riflessioni in tema di decisioni amministrative, intelligenza artificiale e legalità*, in *Federalismi.it*, 7, 2021, 187 ss.; A. Papa, *Intelligenza Artificiale e decisioni pubbliche tra tecnica, politica e tutela dei diritti*, in *Federalismi.it*, 22, 2022, 101 ss; N. Rangone, *Intelligenza artificiale e pubbliche amministrazioni: affrontare i numerosi rischi per trarne tutti i vantaggi*, in *BioLaw Journal*, 2, 2022, 473 ss.; A. Rocca, *L'impatto dell'Intelligenza Artificiale nella Pubblica Amministrazione*, in *ratioiuris.it*, 18 marzo 2024; A. Valsecchi, *Algoritmo, discrezionalità amministrativa e discrezionalità del giudice*, in *iusinitinere.it*, 14 settembre 2020.

[74] N. Cappellazzo, *Algoritmi, automazione e meccanismi di intelligenza artificiale: la classificazione proposta dal Consiglio di Stato*, in *Federalismi.it*, 23 marzo 2022, 1 ss.; C. Filicetti, *Sulla definizione di algoritmo (nota a Consiglio di Stato, Sezione Terza, 25 novembre 2021, n. 7891)*, in *giustiziainsieme.it*, 8 febbraio 2023.

[75] Così ha prescritto il Tar Lazio (sez. III bis, 14 febbraio 2017, n. 3769) in una sentenza relativa all'algoritmo utilizzato per formare le assegnazioni alle sedi di servizio degli insegnanti.

alizzata anche semplicemente vincolando le amministrazioni pubbliche a servirsi solo di *software* di tipo *open source*. Nemmeno così, però, si risolverebbe di per sé il problema della trasparenza algoritmica, non solo perché il codice è difficilmente comprensibile per i non addetti a lavori, ma anche perché non necessariamente riuscirebbe a spiegare le ragioni alla base di una decisione assunta da algoritmi di *machine learning*, progettati per "imparare" dai dati ed evolversi automaticamente di conseguenza[76].

La seconda e più delicata questione da considerare è quella linguistica. Si è già detto di come il linguaggio naturale – e specificamente il linguaggio giuridico, che è intriso di definizioni tecniche specifiche, estranee al linguaggio comune – non siano adeguati alla trasposizione delle regole algoritmiche. Infatti, «la declinazione della trasparenza come "diritto alla spiegazione", e quindi una interpretazione delle norme che tiene conto dell'evoluzione tecnologica, è invero imposta dalla caratteristica, sopra già evidenziata, che accomuna tutti i sistemi algoritmici, ovvero la loro "opacità linguistica", dietro il quale si nasconde il rischio non solo della non comprensibilità, ma anche della non corrispondenza tra ciò che prevede la regola giuridica e ciò che è stato "trasposto" nel linguaggio macchina», che è uno dei 2500 linguaggi di programmazione attualmente disponibili[77].

Eppure, secondo il Consiglio di Stato (sez. IV, 8 aprile 2019, n. 2270)[78] il principio della trasparenza algoritmica implica la «piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico». Quindi occorre che «la "formula tecnica", che di fatto rappresenta l'algoritmo, sia corredata da spiegazioni che la traducano nella "regola giuridica" ad essa sottesa e che la rendano leggibile e comprensibile, sia per i cittadini che per il giudice». In particolare, questa «conoscibilità dell'algoritmo deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti». Solo così, infatti, il giudice potrà «sindacare la stessa logicità e ragionevolezza della decisione amministrativa robotizzata, ovvero della "regola" che governa l'algoritmo». In sintesi, questo ed altri arresti della giurisprudenza amministrativa attraggono l'algoritmo all'interno del concetto di "atto amministrativo informatico" che, in ossequio al principio di trasparenza dell'azione amministrativa, deve essere accessibile da parte dei soggetti interessati[79]. Il problema di fondo di questa decisione è che essa esplicitamente muove dall'erroneo presupposto che, citando la sentenza, «la regola tecnica che governa ciascun algoritmo resta pur sempre una regola amministrativa generale, costruita dall'uomo e non dalla macchina, per essere poi (solo) applicata da quest'ultima»; invece oggi i sistemi di intelligenza artificiale non si limitano ad applicare regole precostituite, ma riescono a produrre regole nuove sulla base dell'esperienza acquisita tramite di processi

[76] A. Corrado, *La trasparenza necessaria*, cit., 210-214; L. Grimaldi, *Costituzionalismo "post-umano"*, cit., 81-82; A. Simoncini*, Il linguaggio*, cit., 27 ss.

[77] G. Lo Sapio, *La trasparenza*, cit., 247.

[78] L. Grimaldi, *Costituzionalismo "post-umano"*, cit., 87-88; B. Marchetti, *La garanzia*, cit., 374-376.

[79] Corrado, *La trasparenza necessaria*, cit., 191. Sulle diverse opinioni dottrinali circa la qualificazione giuridica del *software* algoritmico si veda la ricostruzione di D. Diaco, *Brevi riflessioni sulla natura giuridica del software (a partire da TAR Lazio, sez. III-bis, n. 8384/2023*), in *giustiziainsieme.it*, 26 luglio 2023.

di elaborazione dei dati.

I medesimi principi sono stati espressi da Cons. Stato, sez. IV, 13 dicembre 2019, n. 8472[80], secondo cui occorre sempre garantire «gli elementi di minima garanzia per ogni ipotesi di utilizzo di algoritmi in sede decisoria pubblica: a) la piena conoscibilità a monte del modulo utilizzato e dei criteri applicati; b) l'imputabilità della decisione all'organo titolare del potere, il quale deve poter svolgere la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all'algoritmo». La conoscibilità e spiegabilità dell'algoritmo – declinata in modo analogo rispetto alla sentenza n. 2270 – consisterebbe, dunque, nel verificare se i criteri, le presunzioni e i risultati dell'algoritmo corrispondano ai requisiti e ai propositi prestabiliti per legge o per provvedimento amministrativo, in modo da poter esercitare il controllo sulle regole di funzionamento dell'algoritmo, tenute anch'esse al rispetto dei principi di imparzialità e buon andamento dell'amministrazione. In questo caso, la trasparenza algoritmica assume una "dimensione rinforzata a geometria variabile", in quanto viene diversamente modulata a seconda dei destinatari: un livello di trasparenza maggiore rivolto al funzionario pubblico responsabile del procedimento decisionale o al giudice nel caso di *judicial review* dell'atto amministrativo; un livello più limitato rivolto alla persona su cui ricadono gli effetti della decisione amministrativa[81].

Più o meno in linea con il Consiglio di Stato, la Corte di cassazione (I sez. civ., ord. 10 ottobre 2023, n. 28358) ha ritenuto soddisfatti i requisiti di trasparenza e conoscibilità dell'algoritmo (nella fattispecie, un algoritmo di *rating* reputazionale) nel momento in cui l'utente è posto in condizione di comprendere lo «schema esecutivo dell'algoritmo», cioè la sequenza dei passaggi necessari a raggiungere un risultato, partendo da determinati dati: tali passaggi devono essere «elementari, univoci, di numero finito, operabili in un tempo finito e con risultato unico» e devono essere spiegati all'utente «in modo non ambiguo e in maniera dettagliata» utilizzando i termini della lingua comune e non certo il linguaggio matematico, che l'utente non è tenuto a comprendere. Ma il problema permane: è davvero possibile descrivere senza ambiguità e con un sufficiente livello di dettaglio dei procedimenti matematici in linguaggio comune? E quali indicatori consentirebbero di valutare, in caso di controversie, se tale spiegazione è adeguata? Ad esempio, proprio nel caso di specie il giudice di primo grado (tribunale di Roma) aveva ritenuto che lo standard minimo di trasparenza algoritmica non fosse sodisfatto, poiché la sua descrizione si limitava all'incidenza dei dati presi in considerazione, senza spiegare le modalità con cui si giungeva al risultato finale (cioè, il "peso specifico" dei singoli fattori considerati e i meccanismi di interazione fra loro). Tale obiezione, per quanto non condivisa dalla Cassazione, è indicativa di un problema insolubile: la spiegazione "a parole" dell'algoritmo produce inevitabilmente un certo grado di oscurità e ambiguità.

Del resto, quando vengono utilizzati algoritmi nel processo decisionale pubblico «si finisce per affidare (spesso silenziosamente e quasi surrettiziamente) a sistemisti e progettisti di *software*, anche estranei all'ente, un ruolo rilevante nell'organizzazione amministrativa e nell'azione amministrativa retta, *in parte qua*, da regole tecniche non

[80] G. Lo Sapio, *La trasparenza*, cit., 245 ss.

[81] L. Grimaldi, *Costituzionalismo "post-umano"*, cit., 87.

accessibili (o comunque non intellegibili). Ne emerge l'immagine di un'"Amministrazione invisibile", spettatrice delle decisioni ad essa stessa imputabili e di un "livello normativo clandestino" celato dall'algoritmo»[82]. Si sente spesso affermare, quindi, che il principio di legalità sostanziale dell'azione amministrativa imporrebbe di stabilire per legge i principi e le regole da osservare nella definizione, progettazione e implementazione del sistema algoritmico che conduce alla decisione amministrativa[83]. Occorrerebbero norme «che regolino il rapporto (di controllo) dell'uomo nei confronti della macchina e non il contrario, affinché non si verifichi una vera e propria inversione della dialettica servo-padrone nei rapporti uomo-macchina»[84], incluse norme tecniche, «volte a disciplinare la progettazione degli algoritmi da parte dell'uomo che, se necessario, si spingano
coraggiosamente a prevedere limiti oltre i quali ingegneri, tecnici e informatici non si potranno spingere»[85]. Queste norme dovrebbero avere «un alto livello di malleabilità e adattabilità, che consenta ai singoli di sperimentare un'ampia gamma di versioni e adattamenti della medesima regola, e in un'attuazione *ex ante* di regole tecniche»[86]. Si tratta però di un obiettivo difficilissimo da realizzare, se si considera che il legislatore non dispone normalmente dele competenze tecniche indispensabili a tal fine e che, in ogni caso, la legislazione non riesce a tenere il passo della rapidissima evoluzione tecnologica. Nello stesso tempo, però, «il tentativo di dare una definizione giuridica unica e assoluta a fenomeni malleabili, liquidi, in continua trasformazione come gli algoritmi potrebbe risolversi in un nulla di fatto in quanto la tecnologia non si cura delle partizioni giuridiche e sistematiche: essa semplicemente si diffonde»[87]. Occorrerebbe, allora, trovare il modo di pervenire a una «*governance ibrida*, basata sulla compartecipazione tra *expertise*, tecnica e giuridica, relazione illuminata dal principio di trasparenza, in funzione di partecipazione, di controllo democratico e di legittimità del *decision making process*»[88].

La terza questione riguarda la definizione degli standard cui le amministrazioni pubbliche dovrebbero conformarsi nei casi in cui si servono di algoritmi. Il *Codice dell'amministrazione digitale*[89], in effetti, non offre molte indicazioni utili in tal senso. L'art. 12, si limita a stabilire al c. 1 che «le pubbliche amministrazioni, nell'organizzare autonomamente la propria attività, utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per l'effettivo riconoscimento dei diritti dei cittadini e delle imprese …» e al c. 2 che esse «utilizzano, nei rapporti interni, in quelli con altre

82 P. Otranto, *Riflessioni*, cit., 199.

83 P. Otranto, *Riflessioni*, cit., 199 e 202.

84 C. Colapietro, *Gli algoritmi*, cit., 173.

85 *Ibid.*

86 E. M. Lombardi, *Norma e algoritmo: alcune considerazioni sul nuovo ordine tecnologico*, *in Giustizia Civile.com*, 7, 2020, 10.

87 N. Cappellazzo, *Algoritmi*, cit., 5.

88 L. Grimaldi, *Costituzionalismo "post-umano"*, cit., 95.

89 D.lgs.82/2005 e successive modifiche.

amministrazioni e con i privati, le tecnologie dell'informazione e della comunicazione, garantendo l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni». L'art. 13-bis, c. 2, richiama il Codice di condotta tecnologica, che dovrebbe disciplinare «le modalità di progettazione, sviluppo e implementazione dei progetti, sistemi e servizi digitali delle amministrazioni pubbliche»; tuttavia, al momento in cui si scrive il Codice non risulta essere stato ancora approvato. Il c. 3 del medesimo articolo chiarisce che le amministrazioni pubbliche devono individuare una persona responsabile per la transizione digitale e possono servirsi di esperti «nello sviluppo e nella gestione di processi complessi di trasformazione tecnologica e progetti di trasformazione digitale». Sulla corretta attuazione di tali disposizioni sorveglia l'Agenzia per l'Italia digitale (AgID), istituita dall'art. 14-bis, incaricata anche di emanare «Linee guida contenenti regole, standard e guide tecniche». In particolare, secondo l'art. 71, l'AgID adotta Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione del Codice. Le Linee guida pubblicate finora e disponibili sul sito dell'AgID[90], però, non riguardano la questione della trasparenza algoritmica. Il "Piano triennale per l'informatica nella Pubblica Amministrazione", adottato da AgID a dicembre 2023[91], prevede l'obiettivo dell'aumento della consapevolezza della pubblica amministrazione nell'adozione delle tecnologie di intelligenza artificiale (obiettivo 5.4), per il quale dovranno essere adottate apposite Linee guida entro il 2024. Da ultimo, la "Strategia Italiana per l'Intelligenza Artificiale 2024-2026"[92], elaborata da un gruppo di esperti e pubblicata il 22 luglio 2024, contiene solo un generico richiamo alla necessità di definire «un registro di dataset e modelli, che siano costruiti secondo principi di trasparenza e *fairness*» (p. 15). Dunque, per il momento non sembra che la normativa di settore sia sufficientemente progredita.

Sul piano operativo forse una soluzione, per quanto parziale, al problema di come realizzare la trasparenza algoritmica potrebbe consistere nella definizione, per via normativa, di indicatori e parametri il più possibile condivisi, in base ai quali misurare il livello di trasparenza algoritmica. Qualche indicazione in tal senso potrebbe forse provenire, in un prossimo futuro, dal Centro europeo per la trasparenza algoritmica (ECAT), inaugurato il 18 aprile 2023, che riunisce ricercatori ed esperti nell'ambito dell'informatica, dell'analisi dei dati, dell'intelligenza artificiale e delle scienze giuridiche e sociali, al fine di analizzare il funzionamento dei *software* delle grandi piattaforme e motori di ricerca. Sarebbe però opportuno, come è stato giustamente osservato[93], che venisse istituita a livello nazionale una specifica Autorità indipendente, con funzioni di garanzia nell'utilizzo dei sistemi di IA, così come opportuno potrebbe essere l'utilizzo, da parte delle pubbliche amministrazioni, solo di *software* algoritmici *open source*, in modo che il codice-sorgente sia per principio disponibile per gli interessati.

Una fonte di ispirazione potrebbe essere rappresentata dalle *Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration*, predisposte

[90] AGID, *Linee Guida sull'accessibilità degli strumenti informatici – PA.*

[91] AGID, *Piano triennale per l'informatica nella Pubblica Amministrazione, 2024-2026*.

[92] Dipartimento per la trasformazione digitale, *Pubblicato il documento completo della Strategia Italiana per l'Intelligenza Artificiale 2024-2026*, 22 luglio 2024

[93] A. Papa, *Intelligenza artificiale*, cit., 112.

dallo European Law Institute (ELI) con sede a Vienna[94]: si tratta di un interessante tentativo di integrare la legislazione europea sull'IA nel contesto specifico della pubblica amministrazione, al fine di stabilire alcune solide garanzie per accrescere la fiducia dei cittadini nell'uso della tecnologia da parte dei decisori pubblici. L'idea centrale alla base delle *Model Rules* è una procedura di valutazione d'impatto, volta a valutare la gravità dei rischi dei diversi sistemi di IA. La regola n. 6, in particolare, prescrive il contenuto del rapporto di valutazione d'impatto, che deve contenere diversi elementi riferiti alla trasparenza algoritmica, fra cui la natura e le caratteristiche tecniche del sistema, la selezione dei dati di formazione, convalida e test, il contesto in cui viene utilizzato il sistema, l'interrelazione del sistema con altri sistemi digitali, una valutazione delle prestazioni, dell'efficacia e dell'efficienza del sistema per quanto riguarda agli obiettivi pubblici previsti, una valutazione dell'impatto specifico e sistemico del sistema sui diritti o interessi fondamentali o altri diritti individuali, nonché sulla democrazia, sul benessere sociale e ambientale.

Un'altra esperienza significativa portata avanti nel Regno Unito è l'*Algorithmic Transparency Recording Standard Hub*[95], che ha l'obiettivo di aiutare le organizzazioni del settore pubblico a fornire informazioni chiare sugli strumenti algoritmici che utilizzano e sul motivo per cui li utilizzano. A tal fine, è stato progettato un modello standardizzato per la registrazione e la condivisione delle informazioni[96], da compilare con le informazioni specifiche richieste, accompagnato da una guida[97] per supportare le amministrazioni pubbliche nella compilazione dei rapporti sulla trasparenza algoritmica. Sarebbe forse opportuno sviluppare qualcosa di simile a livello di Unione europea, raggiungendo non solo agli enti pubblici, ma anche a quelli privati.

5. Riflessioni conclusive

È ormai un dato di fatto che tutti noi siamo parte di un ecosistema "tecno-antropologico", se non addirittura "antropo-tecnocratico", nel quale siamo contemporaneamente progettisti-produttori di sistemi tecnologici e destinatari passivi e spesso inconsapevoli della tecnoregolazione. Ciò considerato, nonostante tutte le difficoltà definitorie e applicative esaminate fin qui, risolvere la questione della trasparenza e della comprensibilità dei *software* algoritmici, alla base dei sistemi di IA, è una priorità ineludibile, se davvero si vuole mantenere la persona umana al centro dei processi decisionali, in ossequio e all'imperativo kantiano della persona come fine e mai come mezzo[98]. Del resto, «il principio democratico e il relativo circuito politico- rappresentativo richiedono di rendere noti al cittadino gli elementi tecnici su cui si è fondata la decisione»[99] e quindi

[94] European Law Institute, *ELI Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration*.

[95] *Algorithmic Transparency Recording Standard Hub*, in *gov.uk,* 5 January 2023.

[96] *Algorithmic Transparency Recording Standard*, in *gov.uk,* 29 November 2021

[97] *Guidance for organisations using the Algorithmic Transparency Recording Standard*, in *gov.uk,* 5 January 2023

[98] C. Colapietro, *Gli algoritmi*, cit., 173.

[99] L. Grimaldi, *Costituzionalismo "post-umano"*, cit., 85.

«la trasparenza del *decision making process*, da estendersi alle logiche artificiali che hanno informato la decisione, costituisce un baluardo indispensabile per la legittimità della decisione guidata dall'algoritmo, poiché consente di discernere l'apporto della tecnica dalla valutazione della politica, compensando quel *vulnus* di democraticità che si realizza quando il processo decisionale è delegato, anche solo in parte, alla macchina»[100]. Si tratta di affermazioni indiscutibili in linea di principio ma, come si è evidenziato nelle pagine scritte fin qua, accompagnate da una gran quantità di questioni irrisolte, che si proverà ora a riassumere.

In primo luogo, si è cercato di spiegare come la nozione di trasparenza algoritmica (AT) sia intrinsecamente vaga e ambigua, perché ingloba al suo interno tanto l'idea dell'accessibilità del codice sorgente – che non solo è protetto dal segreto industriale, ma che in ogni caso non chiarisce i procedimenti mediante i quali l'algoritmo produce l'output finale – quanto quella della spiegabilità dei processi algoritmici (xAT). Quest'ultima, peraltro, deve misurarsi con le difficoltà della "traduzione" di procedimenti informatici in enunciati linguistici nonché con il variabile livello di competenza e comprensione delle diverse categorie di interlocutori: esperti tecnici, *deployer* (privati o pubblici) che si servono di algoritmi nell'esercizio delle loro attività o destinatari finali delle decisioni.

In secondo luogo, si è evidenziato come, al momento attuale, la spiegabilità algoritmica risenta della mancanza di standard certi e misurabili attraverso cui poter valutare la sua adeguatezza. L'elevato livello di opacità dei sistemi algoritmici – dovuto in parte anche all'esigenza dei loro produttori di proteggere il segreto industriale – fa che le decisioni, le scelte e le azioni così realizzate siano sostanzialmente "inspiegabili", dal momento che né i destinatari finali né di *deployer* e in certa misura nemmeno i programmatori stessi dei sistemi sono in grado di comprendere le ragioni che hanno dato luogo ad un determinato risultato finale[101]. Però, l'utilizzo di algoritmi da parte delle pubbliche amministrazioni, e quindi la delega del potere decisionale alle macchine, non può essere un alibi per la reintroduzione di nuove forme di "oscurità autoritativa"[102], che può impattare negativamente sull'effettività delle garanzie procedurali e processuali[103]. In un modo o nell'altro, quindi, occorre che i destinatari finali ricevano una esauriente spiegazione dei processi che hanno condotto all'adozione della decisione automatizzata e delle ragioni in base alle quali la pubblica amministrazione ha scelto di accettare o di rifiutare il risultato prodotto dal sistema. Questo, in effetti, è il nodo problematico intorno al quale ruota la giurisprudenza relativa all'utilizzo di algoritmi da parte delle pubbliche amministrazioni, esaminata nel par. 4: i reiterati richiami alla "conoscibilità" dell'algoritmo mediante spiegazioni che traducano le formule tecniche in regole giuridiche si scontrano, infatti, con l'assenza di indicatori standardizzati tali da consentirne la realizzazione in concreto.

Sono stati comunque avviati recentemente alcuni interessanti tentativi per porre rimedio a tale mancanza. Fra questi, sono state richiamate nelle pagine precedenti alcune esperienze tedesche (le *Algo Rules* elaborate nel 2019 dalla Bertelsmann Stiftung),

100 *Ibid.*

101 M. Fasan, *I principi costituzionali*, cit. 186.

102 G. De Minico, *Fundamental Rights*, cit., 31-32.

103 N. Rangone, *Intelligenza artificiale*, cit. 483.

austriache (le *Model Rules* per valutare l'impatto dei processi decisionali algoritmici da parte delle pubbliche amministrazioni, definite dallo European Law Institute), inglesi (l'*Algorithmic Transparency Recording Standard Hub*) e di livello internazionale (il documento, non ancora pubblico, sulla *Transparency taxonomy of AI systems*, recentemente prodotto dall'ISO), mentre l'Italia sembra ancora un po' indietro in questo campo. Si è inoltre messo in luce l'approccio utilizzato dal nuovo regolamento europeo sui sistemi di intelligenza artificiale, che è integrato da allegati che contengono indicazioni piuttosto precise sul tipo e sulla qualità delle informazioni da fornire alle diverse categorie di destinatari (organismi nazionali di supervisione, *deployer* dei sistemi di IA e utilizzatori finali) e che, nella quinta sezione, demanda alla Commissione europea il compito di interagire con gli organismi europei di normazione (CEN, CENELEC, ETSI), al fine di pervenire alla definizione di norme tecniche armonizzate cui adeguare i sistemi di IA.
Va sottolineato, in terzo luogo, che una precondizione per legittimare l'utilizzo dei sistemi algoritmici nei processi decisionali pubblici è l'aspettativa ragionevole – tuttavia non comprovata – che le macchine "intelligenti" siano in grado di differenziare senza discriminare[104]. Altrimenti, la presunta neutralità di tali sistemi potrebbe nascondere pratiche discriminatorie causate da *dataset* viziati da pregiudizi, impedendo in tal modo di identificare, contrastare e sanzionare le discriminazioni perpetrate su base tecnologica. Allora, nel caso di sistemi di IA generativa che producono e processano dati inferiti, bisognerebbe definire dei parametri da applicare per garantire un elevato livello di *fairness* dei dati di partenza e dei procedimenti di elaborazione, tenendo tuttavia presente la necessità di preservare la privatezza dei dati personali.
Non a caso, l'aspetto più interessante dei documenti sopra richiamati relativi agli standard di trasparenza è quello di individuare un metodo operativo per la realizzazione pratica della *fairness* algoritmica, alla quale la questione della trasparenza è strettamente connessa. La *fairness* algoritmica può essere intesa come "equità negativa, ossia come assenza o eliminazione di *bias* che producono o acuiscono forme di discriminazione, ma anche come "equità positiva", fondata sul riconoscimento dell'eguaglianza e del valore morale delle persone, che implica la giustizia distributiva (cioè, l'equa distribuzione di risorse e opportunità), il diritto alla giustificazione (cioè, la tutela dell'uguale diritto di ogni persona di richiedere una giustificazione per il trattamento decisionale algoritmico a cui è sottoposta) e l'uguaglianza di relazione (cioè, il rispetto delle persone come individui particolari anche nel caso di profilazione algoritmica)[105]. Tuttavia, l'idea di equità che viene tenuta per lo più presente nella programmazione della maggior parte degli algoritmi attuali sembra essere affine a quella su cui si basano le democrazie liberali, incentrate sulla difesa dei diritti e delle libertà fondamentali dal potere coercitivo, mentre trovano spazio molto minore le concezioni della giustizia di tipo distributivo[106] o della democrazia ugualitaria[107], fondata sulla realizzazione di condizioni di uguaglianza di fatto attraverso la riduzione dele disparità socio-economiche[108]. Al di là

104 A. Papa*, Intelligenza artificiale*, cit., 107.

105 B. Giovanola – S. Tiribelli, *Equità e decisioni algoritmiche*, in *Teoria*, 2, 2022, 117 ss.

106 J. Rawls, *A theory of Justice*, Cambridge, 1971

107 N. Bobbio, E*guaglianza e libertà*, Torino,1995.

108 A. Santangelo, *Equità degli algoritmi e democrazia*, in *Scientific Journal on Digital Cultures*, 2, 2020, 21 ss.

di sporadici esempi, infatti, alla dimensione della xAT manca «una riflessione condivisa ed eventualmente sindacabile, delle differenti visioni di mondo implicite al concetto di *fairness*»[109]: solo attraverso un substrato valoriale condiviso è possibile programmare algoritmi il più possibile *unbiased*, che contribuiscano a ridurre le discriminazioni e le disparità di trattamento presenti nella società. La trasparenza algoritmica, dunque, può contribuire a rendere palese a quale concezione di *fairrness*, l'algoritmo si ispira.

In conclusione, resta da chiedersi se vi sia qualche appiglio per ancorare la trasparenza algoritmica a principi di rango costituzionale, questione che richiederebbe certamente un approfondimento ben maggiore del contenuto di queste poche righe conclusive. Pur nella consapevolezza dei rischi attinenti alle interpretazioni evolutive della Carta costituzionale[110], non si può non considerare che, se la nostra Costituzione non si adeguerà alle sfide della contemporaneità – come certamente è avvenuto nel momento storico del suo originario concepimento – sarà progressivamente relegata alla marginalità.

Dunque, se lo sviluppo della IA impone di ripensare la persona umana nella sua interezza, di ricollocarla in una diversa dimensione caratterizzata dall'inevitabile relazione con le "macchine sociali"[111], può essere utile rileggere l'art. 2 Cost. alla luce del fatto che gli ecosistemi digitali, in cui gli elementi naturali e quelli tecnologici sono inscindibilmente interconnessi, potrebbero essere considerati oggi come formazioni sociali in cui l'uomo svolge la sua personalità, in cui dunque devono essere garantiti i diritti fondamentali dell'individuo e deve essere richiesto l'adempimento dei doveri inderogabili di solidarietà economica, politica e sociale, gravanti anche sui gestori delle infrastrutture tecnologiche su cui tali sistemi si basano. Peraltro, poiché l'art. 2 Cost. tutela l'individuo all'interno delle formazioni sociali, ma anche le formazioni sociali di per sé, si potrebbe azzardare di fondare sull'art. 2 Cost. anche la garanzia del fatto che i sistemi sociali algoritmici possano continuare a esistere e a svilupparsi. Inoltre, in riferimento all'art. 3 Cost., l'opacità algoritmica rischia sempre più frequentemente di caratterizzarsi come un ostacolo che limita di fatto la libertà e l'eguaglianza dei cittadini, impedendo il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese: infatti, essa può generare disparità, incompatibili con il principio di uguaglianza sostanziale, fra chi possiede gli strumenti cognitivi necessari a comprendere i linguaggi algoritmici e chi non ne dispone; può far sì che molte persone vengano escluse non solo dalla comprensione dei processi decisionali, ma anche dall'accessibilità ai circuiti di *decision making*, producendo un *vulnus* sotto l'aspetto della loro piena partecipazione attiva alla

[109] A. Sterpa e al. *L'ordine giuridico*, cit., 1141.

[110] Solo qualche cenno bibliografico *ex multis* sulla questione dell'interpretazione della Costituzione: M. Betzu, *Interpretazione e sovra-interpretazione dei diritti costituzionali nel cyberspazio*, in *Rivista Aic*, 4, 2012, 1 ss.; E. Di Salvatore, *Interpretazione e nozioni della Costituzione*, in *Costituzionalismo.it*, 1, 2023, 1 ss.; F. Modugno, *Interpretazione costituzionale e interpretazione per valori*, in *Costituzionalismo.it*, 3, 2005, 1 ss.; R. Nania, *Su alcune questioni di metodo nell'insegnamento del diritto pubblico*, in *Nomos*, 2, 2014, 1 ss.; F. Petrillo, L*'interpretazione della Costituzione tra positivismo giuridico della modernità e stato di sicurezza*, in *Società e diritti*, 2, 2016, 138,163; S. M. Pisacane, *Interpretazione costituzionalmente orientata e diritto vivente*, In *LUISS working paper*, 5, 2017; G. Pino, *Interpretazione costituzionale e teorie della Costituzione*, Modena, 2019; G. Pitruzzella, *L'interpretazione conforme e i limiti alla discrezionalità del giudice nell'interpretazione della legge*, in *Federalismi.it*, 3, 2021, 160 ss.

[111] A. Simoncini, *Il linguaggio*, cit., 4.

vita democratica; può esporre le persone a lesioni della loro dignità personale o della loro *privacy*, senza che esse ne siano consapevoli e siano poste in condizioni di avvalersi efficacemente degli strumenti di tutela. Come sostenuto in più occasioni dal Consiglio di Stato, l'opacità algoritmica è contraria ai principi di imparzialità e buon andamento della pubblica amministrazione (art. 97 Cost.), senza contare che l'assenza o la carenza della motivazione della decisione amministrativa causata dall'opacità algoritmica compromette le garanzie processuali, qualora gli interessati vogliano agire in giudizio per la difesa dei propri diritti e interessi legittimi (art. 24 Cost. e art. 6 Cedu). I produttori, gli sviluppatori, i proprietari e persino i *deployer* privati di algoritmi e sistemi di intelligenza artificiale agiscono secondo il principio di libertà di iniziativa economica, di cui all'art. 41 Cost.: poiché quest'ultima «non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla salute, all'ambiente, alla sicurezza, alla libertà, alla dignità umana», non è irragionevole ritenere l'opacità algoritmica un rischio da questo punto di vista (almeno in relazione alla libertà e alla dignità umana, ma probabilmente anche per la sicurezza). Infine, portando il ragionamento all'estremo, anche l'art. 9 Cost. nella sua più recente formulazione riferita alla tutela degli ecosistemi[112], potrebbe prestarsi ad essere applicato ai sistemi di interazione uomo-macchina, che di fatto sono – sempre più saranno in futuro – i moderni ecosistemi in cui si svolge gran parte della nostra vita (il *digital environment*). Pur trattandosi evidentemente di una suggestione assolutamente estranea alle intenzioni degli estensori della legge di revisione costituzionale, in prospettiva futura questa lettura potrebbe essere in qualche modo favorita dal richiamo alla ricerca scientifica e tecnica contenuto nel primo comma dell'art. 9 Cost. e a quello del secondo comma riferito alle future generazioni, che ancora più di quelle attuali saranno plasmate dalla tecnologia. Poiché la tutela di cui all'art. 9 si riferisce agli ecosistemi in sé – quindi a tutte le loro componenti e non a quella umana in particolare – la norma potrebbe prestarsi non solo alla protezione dei diritti individuali all'interno dell'ecosistema digitale, ma anche alla protezione dello sviluppo tecnologico, essenziale alla sussistenza dell'ecosistema stesso.

[112] L. cost. 1/2022 che ha modificato gli artt. 9 e 41 Cost.

La sfida logica (ed ontologica) dei principi costituzionali dinnanzi al linguaggio dell'AI*

Stella Romano

Abstract

Il contributo è percorso da un interrogativo sempre più impellente, ossia, se ed in quali termini sia realizzabile (ed auspicabile) un'impermeabilizzazione delle nostre carte costituzionali alla nuova realtà plasmata dal mondo digitale e se, in tale processo a necessaria osmosi selettiva, è il mondo digitale a doversi adeguare ai principi ed ai valori costituzionali. Al fine di accennare un tentativo di risposta a tale interrogativo, occorre vagliare preliminarmente, attraverso l'ausilio dell'ermeneutica, i processi costitutivi alla base delle tecniche di A.I.; in secondo luogo, con l'ausilio della dogmatica costituzionale si potranno ricostruire le coordinate interpretative che presiedono alla tutela del progresso ed alla definizione dei suoi limiti ed, infine, si procederà alla ricognizione delle tecniche di normazione dell'A.I., al fine di verificarne la compatibilità costituzionale.

The contribution is traversed by an increasingly pressing question, that is, whether and in what terms it is feasible (and desirable) to seal our constitutional documents to the new reality shaped by the digital world and whether, in this process with necessary selective osmosis, it is the digital world having to adapt to constitutional principles and values. In order to outline an attempt to answer this question, it is necessary to preliminarily examine, with the help of hermeneutics, the constitutive processes underlying AI techniques; secondly, with the help of constitutional dogmatics it will be possible to reconstruct the interpretative coordinates that govern the protection of progress and the definition of its limits and, finally, we will proceed with the recognition of the AI standardization techniques, in order to verify their constitutional compatibility.

Sommario

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

Keywords
ermeneutica digitale – principi costituzionali – AI Act – intelligenza artificiale – diritto costituzionale

"Lo vedi il futuro?
È più grande di me e di te".

1. L'ermeneutica quale chiave di indagine privilegiata del linguaggio dell'A.I.: un'analisi preliminare

In un tempo come il nostro in cui le innovazioni della tecnologia sospinte dall'economia, applicate agli aspetti considerati più sacri e indiscutibili della vita, moltiplicano i 'casi estremi', le diverse concezioni del diritto ritornano a mettersi a nudo e la discussione che si accende riporta a galla l'antica tensione tra ciò che è posto e ciò che è giusto. Una tensione che appare nettamente acuirsi con l'opera di re – ingegnerizzazione della realtà sospinta dalle tecniche di intelligenza artificiale, in grado di ridisegnare e ristrutturare il sistema della società e di trasformare profondamente le nostre realtà secondo un ordine ed un significato diverso e singolare[1].
Tale potere radicalmente trasformativo dell'esistente emerge dalla stessa definizione di A.I. contenuta nell'art. 3 del regolamento europeo del 13 giugno 2024 che rappresenta la prima legge europea sull'intelligenza artificiale. Dalla penna del legislatore europeo l'intelligenza artificiale si profila, infatti, quale «sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»[2]. Prendendo le mosse da tale definizione ed

[1] Riflessioni quantomai recenti e profonde sui cambiamenti indotti dall'A.I. su tutte le sfere dell'Umano sono contenute nel libro di R. Kurzweil, *La singolarità è più vicina. Quando l'umanità si unisce con l'A.I.,* Milano, 2024, in cui l'autore utilizza il termine "singolarità", traendolo dal linguaggio matematico, per affermare che la trasformazione prodotta dall'A.I. sarà radicale e condizionerà a tal punto intelligenza e coscienza umana, che sarà difficile comprendere il confine tra le due forme di intelligenza.

[2] Tale definizione è contenuta nel Regolamento europeo sull'intelligenza artificiale n. 1689 del 2024 che ha stabilito regole armonizzate sull'intelligenza artificiale ed era stata preceduta dalla definizione fornita dallo High Level Expert Group on AI, nel rapporto predisposto al fine dell'elaborazione di una strategia europea sull'A.I., dove si elencavano le diverse funzioni dell'A.I. Tale definizione riecheggia, in parte, quella di John Mc Carthy, uno dei pionieri della disciplina dell'intelligenza artificiale che, nel testo *What is Artificial Intelligence,* rapp. tecn., Standford University, 2007, ha definito l'A.I. come «*the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable*».

abbracciando una delle possibili linee o prospettive dell'ermeneutica digitale[3], ossia quella relativa all'indagine sul processo di costituzione dei dati, l'uso dell'intelligenza artificiale interroga *in primis* semiotici e linguisti sui possibili processi interpretativi, su cui si basano i modelli di addestramento dell'A.I.
Chi scrive, infatti, è fermamente convinto della necessità indefettibile di allargare l'ambito di qualsivoglia quesito di natura costituzionale sulle tecniche e gli usi dell'A.I., alle cosiddette teorie ermeneutiche e di trascendere almeno preliminarmente, i sicuri limiti di quello che, in questo lavoro, si vorrebbe definire il livello prettamente giuridico della discussione[4].

1.1. I diversi tipi di apprendimento ed il limite dell'autoevidenza cognitiva del dato.

Data tale premessa, occorre, quindi, procedere alla distinzione di tre livelli nell'ermeneutica dei processi di costituzione di A.I.: l'agente che produce il processo di comunicazione, decisione e/o raccomandazione, il modello interno che questo usa per prendere decisioni e l'algoritmo che crea tale modello partendo dai dati[5]. L'A.I., d'altronde, non può essere riduzionisticamente ricondotta ad una mera sequenza di operazioni algoritmiche imposte dall'uomo, ma essa impara attraverso alcune tecniche di apprendimento che permettono di "incastrare" i dati immessi nella scatola nera delle macchine, attraverso il cosiddetto *data scraping*.
Si è distinto, infatti, tra apprendimento supervisionato, non supervisionato e per rinforzo. Il modello supervisionato consiste nel fornire al sistema informatico una serie di nozioni specifiche e codificate ossia modelli ed esempi che permettano la costituzione di un vero e proprio *database* di esperienze, ossia la matrice a partire da cui la macchina apprende; ne deriva che la macchina è così capace di formulare ipotesi induttive scansionando una serie di problemi specifici, per ottenere una soluzione ad un problema generale[6]. L'apprendimento non supervisionato prevede la codifica preliminare delle informazioni senza alcun esempio di utilizzo dei dati stessi. La catalogazione delle informazioni ed i risultati sono demandati alla macchina stessa, che deve,

[3] L. M. Possati - A. Romele prospettano che ogni ricerca di ermeneutica digitale dovrebbe tenere conto di almeno tre livelli: la prima, per cui ogni riflessione sulla tecnologia dovrebbe partire dalla tecnologia stessa. In tale primo livello di riflessione, si inquadra il pensiero di Possati la cui la tesi centrale considera il software una forma di giudizio riflettente, ossia «un giudizio riflettente digitale». In secondo luogo, l'ermeneutica digitale può essere considerata come un insieme di riflessioni sulle condizioni sociali di produzione e fruizione delle tecnologie digitali e dei loro contenuti. In terzo luogo, l'ermeneutica digitale potrebbe includere riflessioni sulla maniera in cui alcune tecnologie contribuiscono a dare nuova forma a visioni del mondo specifiche. Tali riflessioni sono contenute in *Ermeneutica digitale e i suoi molteplici significati,* in *Critical Hermeneutics*, 4(1), 2020 *Biannual International Journal of Philosophy*.

[4] D'altronde già L. Lessig in *Code and Other Laws of Cyberspace*, New York, 1999 aveva evidenziato come la regolamentazione di condotte individuali, in un contesto come il cyberspazio, potesse svolgersi in modo appagante soltanto previa considerazione della intrinseca peculiarità di questa tecnologia, ossia della sua architettura o meglio del suo *code*.

[5] N. Cristianini, *Machina sapiens, L'algoritmo che ci ha rubato il segreto della conoscenza,* Bologna, 2024.

[6] Sulle varie distinzioni tra i vari tipi di apprendimento si veda la classificazione svolta da G. Sartor, *L'intelligenza artificiale e il diritto,* Torino, 2022.

di conseguenza, autonomamente impartire loro significato e produrre un risultato. A questo livello, è ipotizzabile una forma di autonomia della macchina, che può avvalersi di una certa "libertà" di scelta nell'evidenziare risultati migliori data una situazione. Infine, vi è l'apprendimento per rinforzo che è, grosso modo, la traduzione in campo tecnologico di determinate teorie comportamentiste riguardo l'apprendimento, per cui la macchina orienta il suo *output* in seguito all'immissione di un insieme di azioni, regole e potenziali stati finali ammissibili[7].

Una delle principali caratteristiche di queste tecniche di *machine learning*[8], in particolare di quelle ad apprendimento non supervisionato, riguarda appunto la stretta correlazione con le branche dell'informatica e della statistica. Tali procedure mirano all'estrazione di informazioni. E qui vi è la giuntura tra le tecniche di A.I. e i Big data, ossia enormi raccolte di dati che, per l'appunto, è difficile trattare usando le tecnologie informatiche solitamente impiegate per la gestione dei dati digitali.

Di conseguenza, da una prospettiva ermeneutica, ciò che è maggiormente rilevante è la capacità dei dati di essere modellati secondo una finalità "analitica" (*analytics*), per cui l'estrazione è finalizzata alla definizione di correlazioni e di predizioni[9]. Infatti, i dati sono il risultato di misurazioni o osservazioni e formano la base su cui gli algoritmi intelligenti imparano a predire il mondo. L'A.I. ha bisogno di dati per essere addestrata e pertanto di dati per applicare il suo addestramento[10].

Da un articolo apparso su *Wired Magazine,* il 23 giugno 2008 dal titolo *The end of theory: the data deluges makes the scientific method obsolete*, il direttore Chris Anderson affermava che, nell'epoca del *petabyte,* il metodo scientifico, basato sulla verifica empirica e sulla teoria, potesse essere superato dalla capacità degli algoritmi di razionalizzare i Big data attraverso procedure di *Big Data Analytics e Data mining*, sino a giungere all'elaborazione di una conoscenza previsionale (*Wisdom*), volta a incrementare la capacità previsionale a partire da set di dati sempre più accurati. Maggiori sono i set di dati, maggiore sarà la capacità previsionale.

Al fine del raggiungimento di tale capacità previsionale, l'apprendimento automatico usa diversi metodi: gli alberi di decisione, la regressione statistica, le macchine a vettori di supporto, le reti neurali. Tali metodi differiscono non solo nelle prestazioni predittive ma anche nella capacità di fornire spiegazioni, e spesso si manifesta una tensione tra i due obiettivi: i sistemi tecnologicamente più avanzati sono più opachi, ossia meno capaci di giustificare le proprie decisioni. Se i sistemi quali gli alberi di decisione, fondati su esempi di generalizzazione dell'informazione implicita nell'insieme o classe di addestramento[11] appaiono modelli decisionali esplicabili nei loro processi predittivi, dall'altro, ritroviamo modelli di apprendimento, come quelli calibrati sulle reti neurali che, invece, si strutturano secondo calcoli complessi intesi a riprodurre le correlazioni

[7] L. De Stefano, *Dalla cybernetica al dataismo. Alcune considerazioni su obsolescenza della teoria e intelligenza artificiale nell'epoca dei Big data*, in *scienzaefilosofia.com,* 2018.

[8] Per *machine learning* si intende un sottoinsieme dell'intelligenza artificiale (AI) che si occupa di creare sistemi che apprendono o migliorano le performance in base ai dati che utilizzano.

[9] Anche su tale punto si veda G. Sartor, *L'intelligenza artificiale e il diritto,* cit.

[10] L. Floridi, *Etica dell'intelligenza artificiale, Sviluppi, opportunità, sfide*, Milano, 2022, 69.

[11] G. Sartor, *L'intelligenza artificiale e il diritto,* cit., 48 – 55.

statistiche tra caratteristiche di input e risultati da predire. In tale modo, si realizzano le reti per l'apprendimento profondo (*deep learning*) in grado di apprendere anche da dati non strutturati, in quanto il modello di elaborazione si presenta come una funzione matematica, data dall'interazione di neuroni, la cui attivazione dipende dagli input forniti sotto forma di valori numerici[12]. In quest'ultimo caso, l'opacità del processo decisionale si contrappone all'esigenza di trasparenza che è, invece, imprescindibile laddove il sistema sia utilizzato per funzioni di rilevanza pubblica e siano in gioco valori di rilievo costituzionali, come nel procedimento amministrativo o nell'ambito della giurisdizione, massime in quella penale[13].

Da tali brevi e sintetiche riflessioni di carattere ermeneutico, si potrebbe dire che il dataismo quantitativo e/o statistico schiude ad un altro tipo di procedimento di conoscenza, che sembrerebbe contrapporsi in maniera dicotomica alla pretesa aristotelica, di predire il fenomeno a partire dalle sue cause e principi in favore della mera, presunta, evidenza o autoevidenza operativa del dato. Si assiste, dunque, ad un capovolgimento del principio di *episteme* che contrappone alla struttura del modello logico - consequenziale, tipico altresì della scienza giuridica, a quello dataistico – quantitativo fondato sulla correlazione, su cui si fonda l'intelligenza artificiale.

2. Costituzionalizzare gli algoritmi o digitalizzare la Costituzione?

Tale capovolgimento epistemologico che segue inevitabilmente allo scollamento ontologico, ossia alla sovrascrizione di «un territorio artificiale sovrapposto al territorio naturale e fisico»[14] ha determinato, sotto il profilo ordinamentale, la necessità dell'organizzazione di un sistema decentrato di regole automatizzate e auto applicative[15], non meramente integrative di quelle legali, ma in grado di dar luogo ad un ordinamento speciale rispetto al quale l'intervento degli Stati appare necessariamente sussidiario[16]. Ciò ha siglato la nascita della cosiddetta *lex informatica*[17], che si fonda su diverse forme

[12] In tale sede non possiamo approfondire l'esame delle tecnologie neurali: tuttavia, si riportano le osservazioni di Sartor, cit., per cui l'elaborazione neurale è un'elaborazione "subsimbolica" che non consiste nei simboli del linguaggio ma piuttosto in vettori di numeri.

[13] Sull'esigenza di tutela della trasparenza si veda A. Simoncini, *Il linguaggio dell'Intelligenza Artificiale e la tutela costituzionale dei diritti*, in *Rivista AIC*, 2, 2023, 1 ss.

[14] G. Scaccia, *Il territorio fra sovranità statale e globalizzazione nello spazio economico,* in *Rivista AIC,* 3, 2017, 17. Si veda altresì M. Bassini, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in questa *Rivista,* 2, 2021, 86 ss. che ha sottolineato come i poteri pubblici sono «l'altrove, impossibilitati a predicare la propria sovranità e a estendere l'*enforcement* delle norme giuridiche entro uno spazio idealizzato come territorio separato».

[15] L. Lessing, *The future of Ideas,* New York, 2001, trad.it. *Il futuro delle idee*, Milano, 2006, 125.

[16] M. Betzu, *I baroni del digitale*, Editoriale scientifica, Napoli, 2022, 17 nonché più risalente nel tempo J. Goldsmith - T. Wu, *Who Controls the Internet? Illusions of a Borderless World,* in *Computer and Telecommunications Law Review*, 13, 7, 2006.

[17] Sul punto si confronti lo studio di O. Pollicino - M. Bassini, *The Law of the Internet between Globalization and Localization*, in M. Maduro et al. (eds.), *Transnational Law - Rethinking Law and Legal Thinking*, Cambridge, 2014.

regolatorie dei sistemi digitali, *in primis* la cosiddetta "*co – regulation*"[18], in cui le leggi statali si verrebbero a integrare con una politica di *self – regulation dei soggetti regolati,* laddove questi la evochino ovvero la necessitino[19]. Si potrebbe, quindi, sostenere che le piattaforme digitali siano soggette ad una doppia regolamentazione: se, da un lato, infatti, vi sono i modelli logici ingenerati dai codici e modelli di apprendimento, come specificato nel primo paragrafo, che definiscono la vera e propria «*architectural regulation*»[20], di creazione interna dei contenuti e di gestione dei dati, dall'altro, nel regime di *self–regulation*, vi è quel coacervo di *soft law,* comprensiva dei termini e delle condizioni di servizio, che, sulla base dei valori di fondo della piattaforma, indicano ciò che è consentito e ciò che è vietato al suo interno. Si è così costituito un ordinamento para - giuridico autonomo, che, attraverso le capacità tecniche dimostrate dall'A.I., in termini di analisi dei dati e di elaborazione di modelli predittivi e decisionali ha offerto alle società pubbliche e private, che sviluppano e producono questa tecnologia, la possibilità non solo di conoscere i comportamenti e i desideri delle persone su diversi livelli di azione, ma anche di condizionare le decisioni e le azioni degli esseri umani[21]. Si potrebbe dire, con un'immagine icastica, che lo spazio virtuale ha sostituito il sovrano statale con un "anti–sovrano" tecno-economico[22], smaterializzando l'abitazione della sovranità ed immergendola in un presente "ipertrofico"[23], di cui le nuove tecnologie sono al tempo stesso fattore e prodotto[24].

Se, dunque, la tecnologia detenuta da pochi soggetti ha il potere di produrre decisioni potenzialmente applicabili a qualsiasi sfera dell'esistenza umana - e altresì mezzi per eseguire decisioni – ciò si riverbera in un inevitabile riflesso sull'ordine politico[25] e sulla dimensione costituzionale delle libertà fondamentali[26].

È quel carattere "ambiguo" della modernità descritto da Zygmunt Bauman, una

---

18 A. Simoncini, *La co-regolazione delle piattaforme digitali*, in *Rivista trimestrale di diritto pubblico*, 4, 2022, 1031 ss.

19 T.E. Frosini, *Internet come ordinamento giuridico,* in M. Nisticò - P. Passaglia (a cura di), *Internet e Costituzione*, Torino, 2014, 60.

20 T. Gilliespie, *Custodians of the Internet. Platforms, and the Hidden Decisions that Shape Social Media,* New Haven-London, 2018.

21 Si è recentemente affermato come, in questo contesto, si è perfezionato un passaggio che sembra rilevante per gli studi di diritto costituzionale: da *code is law* a *code as source of law*: così O. Pollicino, Regolazione e innovazione tecnologica nell' "ordinamento della rete", relazione al convegno annuale dell'Associazione Italiana dei Costituzionalisti, Salerno, 15 novembre 2024.

22 M. Luciani, *L'antisovrano e la crisi delle costituzioni,* in *Rivista di diritto costituzionale,* 1, 1996, 124 ss.

23 M. R. Ferrarese, *Il diritto al presente. Globalizzazione e tempo delle istituzioni*, Bologna, 2002, 7 ss.

24 Si confronti anche G. Pascuzzi, *Il diritto dell'era digitale,* Bologna, 2006, 192.

25 A. Simoncini, *La dimensione costituzionale dell'intelligenza artificiale,* Bologna, 2022.

26 Sui cambiamenti prodotti sull'assetto dei poteri e sulla fisionomia dello Stato, si veda L. Torchia, *Poteri pubblici e poteri privati nel mondo digitale*, in *Il Mulino*, 1, 2024, 28, in cui si afferma come: «la sovranità digitale, rispetto alla nozione tradizionale di sovranità, presenta un carattere nuovo, perché viene invocata sia per assicurare la difesa contro interferenze esterne e, quindi, il controllo sul territorio (naturale e digitale) nazionale, sia, innovativamente, per espandere le regole di ciascun ordinamento, che seguono – per così dire – i cittadini di quell'ordinamento: per le regole sulla privacy sinora, e potenzialmente per la nuova regolazione europea in materia di mercati e servizi digitale e di intelligenza artificiale, gli obblighi imposti hanno una proiezione extraterritoriale» nonché O. Pollicino, *Potere digitale*, in M. Cartabia - M. Ruotolo (a cura di), *Potere e Costituzione*, in *Enciclopedia del Diritto*, V, Milano, 2023.

«combinazione agghiacciante e poderosa di impalpabilità e onnipotenza, non fisicità e potere di determinare la realtà»[27] e, che sembra percorrere come un *fil rouge* la prima legge europea in materia di intelligenza artificiale.

Il compito che attende il diritto costituzionale di fronte agli scenari inediti delineati dallo sviluppo delle tecniche e dei sistemi di A.I. appare, quindi, radicalmente "trasformativo", soprattutto nella misura in cui intenda sconfinare le colonne d'Ercole dell'antropocentrismo e considerare l'emersione di una intelligenza nuova aliena e tutelabile in relazione quanto alle sue capacità decisionali ed altresì alla tipologia di procedimento logico interno per giungervi.

Ci si è chiesti, dunque, se occorra uno sforzo concettuale al fine di adeguarsi al nuovo contesto determinato dalla tecnologia digitale[28], riconsiderando e riadattando le categorie del costituzionalismo «alla luce dei cambiamenti prodotti dall'erompere della tecnologia nelle nostre vite e nelle nostre comunità, in quella che è stata definita «la nuova civiltà digitale»[29]. Una parte della dottrina ha, infatti, parlato di "costituzionalismo digitale"[30], assegnando alla fonte costituzionale la funzione di adattare i suoi valori alla società digitale, liberandola dai vincoli della dimensione statale e così illuminandone la transizione verso «*new values and ideals, like it happened when constitutionalism eventually became 'democratic*»[31].

Ciò che tenteremo di fare, seppur con poche pennellate e senza pretesa di esaustività alcuna, è verificare, quindi, se ed in quali termini sia realizzabile (ed auspicabile) un'impermeabilizzazione della Costituzione alla nuova realtà plasmata dal mondo digitale e se, in tale processo a necessaria osmosi selettiva, è il mondo digitale a doversi adeguare ai principi ed ai valori costituzionali[32].

2.1. L'ordine pubblico costituzionale in bilico tra tutela del progresso e garanzia dei diritti

In tale quadro, se osserviamo con attenzione il nostro ordine pubblico costituzionale, da un lato, possiamo rinvenire un primo blocco di valori costituzionali che presiedono alla costituzionalizzazione del valore che l'intelligenza artificiale apporta all'innovazione ed al progresso; dall'altro, nello stesso tessuto costituzionale, si può scorgere l'addentellato costituzionale su cui si edifica la necessità imprescindibile di apporre solidi argini ai rischi ai diritti fondamentali insiti nell'uso delle tecniche di intelligenza

[27] Z. Bauman, *Globalization. The Human Consequences,* Columbia University Press, New York, 1998, trad. it, *Dentro la globalizzazione. Le conseguenze sulle persone,* Roma Bari, 1999, 23.

[28] A. Simoncini - S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 1, 2019, 87 ss.

[29] Si vedano, in particolare, le riflessioni di T.E. Frosini, *Il costituzionalismo nella società tecnologica,* in *Il diritto dell'informazione e dell'informatica*, 3, 2020, 465 ss.

[30] Sul punto si vedano le riflessioni G. Teubner., *Breaking Frames: economic globalisation and the emergence of the lex mercatoria*, in *European Journal of Social theory*, 2002.

[31] E. Celeste, *Digital constitutionalism: a new systematic theorization,* in *International Review of Law, Computers e Technology,* 33, 2019, 88 ss.

[32] In tali termini, si esprime lo stesso F. Ballaguer Callejon, *La Costituzione dell'Algoritmo,* Firenze, 2023.

artificiale, al fine di conformare un progetto umano per l'era digitale che, potremmo dire, ancora manca[33].

Tra le prime disposizioni, a comporre il mosaico costituzionale a tutela del valore del progresso scientifico sotteso all'apporto tecnologico dell'intelligenza artificiale, vi rientrano l'art. 4 della Costituzione, che afferma il riconoscimento del diritto al lavoro e l'art. 9 Cost., con cui la Repubblica promuove lo sviluppo della cultura e della ricerca scientifica e tecnica; l'art. 21 Cost., che, proclamando la libertà di espressione, consente l'esplicazione dell'attività di creazione e divulgazione dell'opera intellettuale e l'art. 33 Cost., sulla libertà dell'arte e della scienza.

In particolare, dalla lettura sistematica delle norme costituzionali, emerge come la garanzia costituzionale della ricerca scientifica non si possa intendere affermata nell'interesse esclusivo del singolo, in una prospettiva meramente individualistica, ma per l'appunto, rappresenti un presupposto indefettibile ed irrinunciabile al fine di soddisfare l'ispirazione degli individui alla conoscenza e per consentire l'avanzamento della società intera. Ciò avviene attraverso il riconoscimento della libertà della ricerca scientifica apprestato dall'art. 33 Cost. che proclama, per l'appunto, una libertà innominata, alla quale non potrà che assegnarsi una regolazione che, per la natura intrinseca della scienza, ivi compresa quella mediata dalla tecnologia digitale, dovrà atteggiarsi quale preventiva[34].

Al medesimo tempo, il volto costituzionale della promozione della cultura e della ricerca non potrà che passare logicamente dalla previa salvaguardia dei nostri valori umani e culturali, come suggerito dall'uso della parola "tutela", che impone ai poteri pubblici di offrire impulso alle nuove scoperte scientifiche, che potranno sfociare nella produzione di beni, a loro volta (auspicabilmente) da salvaguardare e valorizzare[35].

La promozione presuppone *ex necesse* una tutela delle fondamenta stabili dei valori costituzionali. In altri termini, il principio informatore di cui all'art. 9 della Costituzione suggerisce la via per risolvere quella tensione potenzialmente irrisolvibile tra l'inevitabile assimilazione dei benefici delle nuove potenzialità offerte dall'intelligenza artificiale e, al contempo, la mitigazione dei potenziali rischi ai diritti fondamentali, ossia, promuovendo queste tecnologie ed evitando al contempo il loro uso improprio, sottoutilizzo o impiego dannoso[36]. Ciò è ben definito ai considerando di apertura (numero 4 e numero 5) del regolamento europeo in cui si specifica che l'uso dell'A.I. può fornire vantaggi competitivi fondamentali alle imprese e condurre risultati vantaggiosi sul piano sociale e ambientale, ma al contempo si sottolinea come la stessa rapida evoluzione della tecnologia insita nell'uso dell'A.I. possa, comportare rischi e pregiudizi, compreso il pregiudizio fisico, psicologico, sociale o economico.

La dimensione dinamica che sospinge l'innovazione tecnologica si infrange sullo

---

[33] L. Floridi, *Etica dell'intelligenza artificiale*, cit.

[34] M. Luciani, *Può il diritto disciplinare l'Intelligenza Artificiale? Una conversazione preliminare*, in *Bilancio Comunità Persona*, 2, 2023, 10 ss.

[35] M. Ainis, M. Fiorillo, *L'ordinamento della cultura*, *Manuale di legislazione dei beni culturali,* Milano, 2022 in cui ampia trattazione viene riservata alla ratio esplicativa della prima parte della Costituzione, dove trovano spazio le istanze di tutela e libertà della cultura.

[36] Sulla responsabilità sociale della scienza si veda H. A. Mieg (ed.), *The Responsibility of Science*, Berlino, 2022.

schermo statico della tutela dei principi e dei valori fondamentali che dovrebbe riverberarsi in tecniche di normazione che tengano conto dei principi - guida per un design *etico* della rivoluzione digitale, come diremo più avanti. Tale interpretazione non può che trovare conforto soprattutto nel quadro d'attuazione dei principi e valori costituzionali, collocati nella prima parte della Costituzione e mi riferisco ai doveri inderogabili di solidarietà politica, economica e sociale sanciti dall'art. 2 Cost., nonché al valore ed al principio della libertà dell'iniziativa economica sancito dall'art. 41 collocato nella parte I, titolo II, relativo ai rapporti economici[37].

Infatti, se ci si colloca sul principio della libertà di impresa, da un lato, occorre sottolineare come al suo interno non si individui esclusivamente la libertà di impresa, in quanto tale, ma qualsiasi attività economica corrispondente all'esercizio di un "fascio di libertà" fra cui la libertà di disporre dei beni, la libertà di investire i capitali, la libertà di destinarli alla produzione o allo scambio di beni o servizi o all'acquisizione di ricchezza, la libertà contrattuale, il potere di organizzare il processo produttivo. A tale principio di libertà non può che essere ricondotta l'attività economica, per l'appunto latamente intesa, dei fornitori di servizi di A.I., delle piattaforme quali portatori della linea editoriale e di organizzazione dei modelli di apprendimento di A.I. Al medesimo tempo, a fornire i confini del principio di libertà di impresa, vi è certamente la definizione dei suoi limiti, pure previsti dal testo costituzionale, per cui la dottrina, sin da epoca assai risalente, ha affermato che il secondo comma dell'art. 41 della Costituzione faceva corpo con la proclamazione di libertà del 1° co. cosicché quei limiti incidono concretamente sulla configurazione della situazione soggettiva di libertà. Essi primariamente non possono che trovare la loro raffigurazione nel principio oggettivo di solidarietà che comanda a chi esercita un diritto di libertà di tenere conto anche del bene comune[38], nonché, per quanto concerne la sfera soggettiva del singolo utente, fruitore di A.I., del valore della dignità e del diritto all'autodeterminazione cristallizzati all'art. 2 della Costituzione e del diritto alla salute ed alla sicurezza sul lavoro garantiti dall'art. 32 della Costituzione.

Più dubbia (in quanto poco ancora inesplorata) appare, invece, la compatibilità della capacità generativa di "comunicazione" delle tecniche di intelligenza artificiale con l'alveo di tutela offerta dall'art. 21 della Costituzione, che assicura a «tutti» la libertà di «manifestare liberamente il proprio pensiero con la parola, lo scritto ed ogni altro mezzo di diffusione». Ciò in quanto, preliminarmente, è arduo fornire aprioristicamente dal punto di vista costituzionale una completa definizione dell'oggetto della libertà, che aiuti a specificare ed articolare quel concetto di manifestazione del pensiero che il Costituente ha voluto esprimere, con intenzione, in termini così generali.

[37] Quanto al valore della solidarietà in generale occorre ricordare le osservazioni di G. Oppo in *Scritti Giuridici*, I, *Diritto dell'impresa*, Padova 1992, 30 ss. da cui cito nonché F. Polacchini, *Doveri costituzionali e principio di solidarietà*, Bologna, 2016.

[38] Sulla solidarietà insieme all'inviolabilità come criteri orientatori della Costituzione democratica v. M. Fioravanti, *Art. 2 Costituzione italiana*, Roma 2017: in particolare, sui doveri inderogabili dell'art. 2 Cost. che sono riferibili, tra gli altri, ai doveri di solidarietà economica evidenziata dai c. 2 e 3 dell'art. 41 Cost. Il rapporto tra gli artt. 2 Cost. e 41, c. 2, è richiamato anche da N. Irti in *L'ordine giuridico del mercato*, Roma-Bari 1998, 85 ss. che definisce i doveri di solidarietà come criteri conformatori dell'iniziativa economica e sottolinea l'opportunità di positivizzare tali doveri.

Per quanto qui interessa, è ormai dato pacifico, in dottrina e in giurisprudenza, che la garanzia dell'art. 21 copre, in via di principio, le manifestazioni di pensiero «divulgate» con la parola, lo scritto e ogni altro mezzo atto a diffondere le espressioni della personalità dell'autore[39]. Il carattere della divulgazione ha riguardo al grado di esternazione dell'oggetto della comunicazione, che vuole trascendere una dimensione privata e riservata per rivolgersi ad uno spazio aperto, laddove i destinatari della comunicazione possono essere in potenza molteplici. Al medesimo tempo, sotto un profilo ontologico, si è autorevolmente affermato che la garanzia costituzionale copre, nello stesso modo, qualunque "messaggio" si intenda diffondere[40]. La tesi della "materia privilegiata", avanzata in dottrina, di una differenziazione della protezione costituzionale in relazione ai contenuti del messaggio «pur logicamente attendibile e rispondente ad esigenze sulle quali si deve convenire, sembra urtare contro la formulazione dell'art. 21 che non autorizza l'interprete a differenziare qualità e quantità dei limiti a seconda della diversa materia costituente l'oggetto delle varie manifestazioni»[41]. In altri termini, la stessa evoluzione e progressiva commistione delle modalità espressive del pensiero hanno reso impossibile la chiara identificazione e identificabilità di categorie concettuali e materie separate, rendendo ininfluente la modalità espressiva e il contenitore del messaggio rispetto al contenuto dello stesso[42]. Rigettata, dunque, dogmaticamente e preliminarmente, la possibilità di arbitrarie discriminazioni all'interno della concezione del diritto di manifestazione del pensiero, occorre rilevare, in positivo quale contenuto assuma nell'interpretazione dottrinale e giurisprudenziale quel concetto di «pensiero», indefinitamente denso di significati, al fine di comprendere se ed in quali termini anche la *cogitatio* della macchina pensante possa rientrare nell'ambito dell'oggetto di tutela dell'art. 21 della Costituzione.

Nonostante la disposizione costituzionale faccia riferimento alla manifestazione del «proprio pensiero», sin da tempo risalente, l'attività interpretativa della Corte costituzionale ha portato ad includere in tale espressione anche «la semplice affermazione di un fatto e la diffusione di una notizia»[43]. Lo *ius narrandi* è, infatti, il diritto di trasmettere notizie e riferire pensieri prevalentemente altrui: «è ovvio che la libertà di pensiero comprenda anche quella di riferire il pensiero altrui, come fatto, o avvenimento della vita»[44]. In questi termini e, depurato della mera matrice emotivo – esistenziale il concetto di pensiero restrittivamente inteso quale oggetto di tutela, ed ampliando l'orizzonte ermeneutico al polo passivo del sistema informativo, privato e pubblico, istituzionale e non della comunicazione di pensiero, si staglia la "libertà di essere informati" quale

[39] A. Pace, *Problematica delle libertà costituzionali*, *Parte speciale. Appendice di aggiornamento*, Padova, 2002. Per una riflessione completa sul valore della libertà di pensiero si veda anche P. Ridola, *Diritti fondamentali. Un'introduzione*, Torino, 2006, 86 ss.; P. Caretti, A. Cardone, *Diritto dell'informazione e comunicazione nell'era della convergenza*, Bologna, 2019, 17 ss.

[40] P. Barile, *Libertà di manifestazione del pensiero*, Milano, 1975.

[41] V. Crisafulli, *In tema di limiti alla cronaca giudiziaria*, in *Giur. cost*, 1965.

[42] A. Pace – M. Manetti, *Art. 21,* in *Commentario della Costituzione*, Bologna, 2006.

[43] Corte cost., sent. 94/1977.

[44] P. Barile, *Libertà di manifestazione del pensiero*, cit.

«risultato sociale dell'esercizio delle libertà di pensiero e di stampa»[45]. Questa impostazione muove, in particolare, dalla ricostruzione dell'attività informativa in termini di rapporto giuridico di comunicazione: da qui la necessità di riconoscere giuridicamente la posizione soggettiva di entrambi i poli, affinché di rapporto si possa parlare.
Tale ricostruzione dogmatica, dettata anche dalle trasformazioni sociali, che sempre alimentano e fondano il diritto, contribuisce a reinterpretare il paradigma dell'art. 21 per cui, nel momento in cui si dà alla norma costituzionale «il significato di una garanzia della libertà di informare, abbiamo compiuto un salto qualitativo rispetto alla semplice libertà di pensiero perché abbiamo già caratterizzato il dettato costituzionale non semplicemente in funzione dell'interesse di chi utilizza il mezzo di diffusione, ma altresì in funzione dell'utilità di un prevedibile destinatario della comunicazione»[46]. La norma costituzionale, per questa tesi, avrebbe pertanto «riguardo ad una manifestazione del pensiero che diventa veicolo di un messaggio immediato, strumento di coesione e di crescita della collettività» [47]. In ogni caso, al di là delle difficoltà dogmatiche che oscillano tra la qualificazione della «libertà di informarsi» come diritto soggettivo o mero interesse, si può comprendere tale situazione giuridica soggettiva «tra le espressioni della personalità individuale» individuandone il fondamento nell'art. 10 della Convenzione EDU, la cui copertura costituzionale sarebbe comunque offerta dall'art. 2 Cost[48] e dal superiore principio democratico, per cui «libertà di manifestazione del pensiero, libertà di discussione e di propaganda, libertà di informazione - nel duplice senso di informare e di essere informati -sono [...] condizioni necessarie per il buon funzionamento, e si può dire per l'esistenza del regime democratico» [49].
Assunto, quindi, che "il diritto di essere informati" non gode di un'autonoma tutela costituzionale rispetto all'art. 21 della Costituzione, i più delicati nodi interpretativi si pongono con riferimento alla fisionomia stessa delle tecniche di intelligenza artificiale gestite dalle diverse piattaforme digitali[50], calibrate su un proprio apprendimento autonomo, fondato su uno specifico bagaglio epistemologico, che trae inferenze dalla conoscenza codificata o dalla rappresentazione simbolica del compito da risolvere. Una fisionomia che appare ancor più complessa laddove si faccia riferimento all'A.I. generativa, ultima frontiera dell'intelligenza artificiale, imperniata sui cosiddetti modelli fondativi e capace di generare una grande quantità di output e di essere applicata ad

[45] G. Gardini, *Le regole dell'informazione*, II ed., Milano, 2009, 35 ss.

[46] N. Lipari, *Libertà di informare o diritto ad essere informati ?,in Dir. radio diff. e telecom.*, 1978, 2, I.

[47] *Ibid.*

[48] C. Chiola, *L'informazione nella Costituzione*, Padova, 1973.

[49] M. Mazziotti, *Appunti sulla libertà di manifestazione del pensiero nell'ordinamento italiano*, in Aa. Vv., *Scritti in onore di V. Crisafulli,* Padova, 1985, II, 517 ss.

[50] Sul tema del rapporto tra potere privato ed informazione si veda: V. Zeno- Zencovich, *La libertà d'espressione. Media, mercato, potere nella società dell'informazion*e, Bologna, 2004; J.M. Balkin, *Old-School/New-School Speech Regulation*, in *Harvard Law Review*, 127(8), 2014, 2296 ss.; C. Caruso, *La libertà di espressione in azione. Contributo a una teoria costituzionale del discorso pubblico*, Bologna, 2014, 81 ss.; G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in questa *Rivista,* 1, 2018, 19 ss.; G.E. Vigevani, *Informazione e Potere*, in *Enc. Dir.*, *I tematici V*, Milano, 2023, 219 ss. e dello stesso autore *Piattaforme digitali private, potere pubblico e libertà di espressione*, in *Diritto costituzionale*, 1, 2023, 41 ss.

una diversa e variegata quantità di contesti[51].

Rispetto a tali modalità di comunicazione, potenzialmente generatrici di disinformazione e finanche di manipolazione[52], si è già evidenziato da parte di autorevole dottrina come possano risultare del tutto inefficaci gli strumenti di repressione inibitoria calibrati sul tradizionale mezzo della stampa in quanto scontano il limite tecnico dato dalla struttura stessa della tecnologia della intelligenza artificiale. Appare, inoltre, estremamente debole e poco effettivo il rimedio proposto dal legislatore europeo nell'AI ACT laddove classifica questa tecnologia come a «rischio limitato», sottoponendola solo agli obblighi di trasparenza, come l'inserimento della dicitura "*deepfake*[53]" nella presentazione del contenuto

Si ritiene, invece, che, in fase di sviluppo della tecnologia, l'*enforcement costituzionalmente adeguato* potrebbe risiedere nella manomissione alterativa (del "modo di pensare") della macchina (della stessa *Weltanschauung* della *machina*, se si potesse dire, o del suo equivalente robotico). Una sorta di *habeas mentem* dell'entità robotica[54]. In tale direzione, quale rimedio *ex ante*, parrebbe muoversi la timida indicazione, pure contenuta nell'A.I. Act laddove si riferisce ad una sorta di alfabetizzazione in materia di A.I. che dovrebbe dotare i fornitori, i deployer ed i fruitori delle misure necessarie per comprendere la corretta applicazione degli elementi tecnici durante la primigenia fase di sviluppo del sistema di A.I., nonché delle misure da applicare durante il suo utilizzo e delle modalità consequenziali adeguate al fine di interpretare l'output del sistema di A.I. Nella fase finale di utilizzo e di fruizione delle tecniche di A.I., di converso*, l'habeas mentem* potrebbe tradursi nei cosiddetti *codici di condotta*, tipici strumenti normativi di co-regolamentazione predisposti dal GDPR (art. 35) e richiamati dal Digital Service Act[55], il Regolamento sui servizi digitali, che trovano la loro base normativa nell'accordo volontario tra attori pubblici e privati e, che stabiliscono meccanismi di responsabilizzazione volontaria delle piattaforme nella gestione dei contenuti, ai fini di protezione dei consumatori e degli utenti. A tali strumenti, il legislatore europeo, nel principale atto di regolamentazione dei servizi digitali, ha affiancato anche altre misure di *soft regulation;* alcune già note, come le "norme volontarie" stabilite dai "competenti organismi di normazione europei e internazionali" (art. 34); altre innovative, quali i "protocolli di crisi" (art. 37), una nuova fonte, dalla non agevole qualificazione, prevista per affrontare circostanze straordinarie che incidono sulla sicurezza o salute pubblica (39). La redazione di tali protocolli — atti di co-regolazione "atipici" — è avviata dalla Commissione e prevede

[51] Per la definizione di modelli fondativi, si veda: R. Bommasani et al., *On the Opportunities and Risks of Foundation Models*, arXiv, 2022.

[52] Si veda, in particolare, O. Pollicino-P. Dunn, *Intelligenza Artificiale e Disinformazione*, Milano, 2024 nonché F. Romero Moreno, *Generative AI and deepfakes: a human rights approach to tackling harmful content*, in *International Review of Law, Computers & Technology*, 2024, 1 ss.

[53] *Deep fake*: un'immagine o un contenuto audio o video generato o manipolato dall'AI che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona.

[54] U. Ruffolo, *Piattaforme, A.I. generativa e libertà di (formazione e) manifestazione del pensiero. Il caso ChatGPT*, in *Giur. It.*, 2024, 2, 472 (commento alla normativa) si veda il contributo del medesimo autore in C. Pinelli - U. Ruffolo (a cura di), *I diritti nelle piattaforme,* Torino, 2023.

[55] DSA: regolamento (UE) 2022/2065 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

il coinvolgimento, nella fase di elaborazione, sperimentazione ed applicazione, delle stesse piattaforme online nonché, laddove necessario, delle organizzazioni della società civile. Su questa direttrice, dinnanzi alla possibilità, ad esempio, di violazioni dei diritti fondamentali ovvero alla alterazione del dibattito civico da parte delle grandi piattaforme online, la Commissione può invitare le stesse — assieme ad altre piattaforme, nonché alle organizzazioni della società civile e altre parti interessate — a partecipare all'elaborazione dei codici di condotta, «stabilendo impegni ad adottare misure specifiche di attenuazione dei rischi nonché un quadro di comunicazione periodica sulle misure adottate e sui relativi risultati». Nella prospettiva, dunque, della moderazione dei contenuti, mediante la co-regolazione si tenta di correggere la profonda asimmetria informativa esistente tra regolatore e regolato, assegnando alla decisione di matrice pubblica, la fissazione dei valori e degli obiettivi generali e coinvolgendo invece nella fase di esecuzione-attuazione i destinatari delle norme[56].

Conclusivamente, la stessa dogmatica costituzionale, seppur tratteggiata con veloci pennellate, mostra che nel denso articolato delle norme costituzionali si possa ritrovare un criterio ordinatore dei valori in gioco messi in chiaro dalle tecniche di intelligenza artificiale. In ultima analisi: il disegno, la costruzione, l'applicazione, la supervisione ed il controllo dei mezzi informatici basati sull'intelligenza artificiale devono osservare i principi costituzionali e i diritti fondamentali come garanzia di protezione diretta o indiretta della persona ed al medesimo tempo assicurare lo sviluppo dell'attività d'impresa sotto l'egida dei principi di sostenibilità ed intelligibilità digitale.

3. Tecniche di regolazione dell'intelligenza artificiale *costituzionalmente orientate*? Tra AI Act e prospettive *de iure condendo*

Tracciato il quadro costituzionale, seppur sintetico, dei principi in materia di A.I., occorrerebbe verificare se, allo stato dell'arte, l'ordine normativo vigente, altresì in una prospettiva multilivello, sia effettivamente espressivo dei principi-valori dinnanzi richiamati. Negli ultimi decenni, sono sorti, infatti, differenti strumenti regolativi di nuova generazione, quali, ad esempio, la cosiddetta soft law ovvero l'adozione di codici etici o di strumenti normativi quali le linee guida o le c.d. *best practices*: fonti sicuramente di struttura ed efficacia diversa rispetto alle fonti primarie tipiche dello strumentario costituzionale.

Il regolamento europeo sull'intelligenza artificiale ha scelto, infatti, come impostazione regolativa il cosiddetto *risk-based approach*: assetto ispirato a forme di normazione ben differenti da quella classica e corrispondente ad una categorizzazione di differenti livelli di rischio associati alle applicazioni di A.I., cui corrisponde specularmente una graduazione della severità dei regimi giuridici applicabili. Il modello adottato dal legislatore è, quindi, calibrato sul rischio nella misura in cui distingue tra gli usi dell'intelligenza artificiale che creano rispettivamente un rischio inaccettabile, un rischio alto

[56] A. Simoncini, *La co-regolazione delle piattaforme digitali*, in *Riv. trim. dir. pubbl.*, 4, 2022 nonché G. Mobilio, *La co-regolazione delle nuove tecnologie, tra rischi e tutela dei diritti fondamentali*, in *Osservatorio sulle fonti,* 1, 2024.

e un rischio basso o minimo, imponendo connessi obblighi e responsabilità, con un apparato sanzionatorio prettamente pecuniario e calibrato sul fatturato annuo globale nell'esercizio finanziario precedente della società che ha commesso l'illecito.
Il primo livello è così costituito da quei sistemi di A.I. considerati capaci di impattare così severamente sui diritti individuali da essere vietati *tout-court*. Le pratiche vietate includono, tra l'altro, l'immissione sul mercato o la messa in servizio di determinati sistemi di riconoscimento biometrici, sistemi di social scoring, sistemi che utilizzino tecniche subliminali per condizionare le scelte di persone o gruppi di persone con l'effetto o rischio di provocare loro un danno. Il secondo livello è costituito, invece, dai sistemi di A.I. categorizzati come "ad alto rischio", individuati sulla base della normativa vigente in materia di sicurezza dei prodotti ovvero sulla base dell'Allegato III dello stesso Regolamento, il quale include in particolare i seguenti settori: biometria; infrastrutture critiche; istruzione e formazione professionale; occupazione, gestione dei lavoratori e accesso al lavoro autonomo; accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi; attività di contrasto; migrazione, asilo e gestione del controllo delle frontiere; amministrazione della giustizia e processi democratici. Tale categoria di rischio rappresenta, peraltro, la più rilevante nell'economia dell'intero Regolamento, in quanto ad essa è dedicata la maggioranza delle disposizioni normative volte a prevedere tutta una serie di obblighi, specie con riferimento ad una valutazione del rischio *ex ante*, da effettuare prima dell'immissione del prodotto sul mercato, per provare a prevenire i rischi connessi all'uso di sistemi di intelligenza artificiale applicati ad aree assai sensibili, come la sorveglianza biometrica, la giustizia ed i servizi sanitari in cui maggiore è il rischio di compromissione del rispetto dei diritti fondamentali della persona.
Il terzo livello è rappresentato da alcuni sistemi di AI che presentano un rischio minimo a cui si applicano, in particolare, obblighi di trasparenza meno onerosi rispetto a quanto richiesto per i sistemi c.d. ad alto rischio. È il caso, ad esempio, dei deep fake o dei contenuti generati da chatbots, che presentano un rischio di personificazione e di conseguente confusione tra umano e AI.
Infine, vi è il quarto livello che, essendo composto da filtri AI di raccomandazione di contenuti e da filtri spam impiegati nella gestione della posta elettronica, si caratterizza per l'assenza di una specifica regolazione a riguardo.
In ultima analisi, un ulteriore profilo di rischio è quello posto dai modelli di AI per finalità generali con rischio sistemico. I modelli di AI per finalità generali sono quei modelli addestrati con grandi quantità di dati, utilizzando l'autosupervisione su larga scala, caratterizzati da una generalità significativa ed in grado di svolgere con competenza un'ampia gamma di compiti distinti.
In base all'art. 53 della legge europea sull'AI, i fornitori di modelli di AI per uso generale devono documentare le informazioni tecniche sul modello al fine di fornire tali informazioni su richiesta all'Ufficio AI ed alle autorità nazionali competenti (art. 53, par. 1, lett. a)) e metterle a disposizione dei fornitori a valle (art. 53, par. 1, lett. b)). Devono inoltre mettere in atto una politica per conformarsi al diritto dell'Unione in materia di diritto d'autore e diritti connessi (art. 53, par. 1, lett. c)) e redigere e mettere a disposizione del pubblico una sintesi sufficientemente dettagliata dei contenuti utiliz-

zati per la formazione del modello (art. 53, par. 1, lett. d)). Inoltre, l'AI Act ha previsto un'ulteriore categoria di rischio specifico, ossia il rischio sistemico, per le capacità di impatto elevato dei modelli di AI per finalità generali, a causa della loro portata e degli effetti negativi effettivi o ragionevolmente prevedibili sulla salute pubblica, la sicurezza, i diritti fondamentali o la società nel suo complesso. In questo caso, i fornitori dovranno anche effettuare valutazioni atte ad individuare e attenuare il rischio sistemico, documentare e notificare incidenti gravi e garantire elevati standard di cybersicurezza sul modello e sulla sua infrastruttura.

La classificazione del rischio, dunque, adotta un approccio tipicamente procedurale, laddove, evidenziato il modello di AI e determinato l'impatto sui diritti fondamentali in un determinato contesto, il legislatore europeo incentra il suo focus sui peculiari obblighi di trasparenza e sulla mitigazione dei rischi sistemici, senza, tuttavia, fornire indicazioni specifiche sul sistema di garanzie effettive e, dunque, di responsabilità connesse ad un uso improprio delle tecniche di AI. Si è, infatti, sostenuto come la valutazione d'impatto sui diritti fondamentali, il cosiddetto FRIA, soffra di carenze strutturali, in quanto calibrato su un esercizio di autovalutazione da parte degli attori pubblici e privati, incaricati dell'implementazione dei sistemi di AI, che, senza un adeguato livello di *enforcement* e armonizzazione, rischiano di divenire meri esercizi burocratici, che duplicano i controlli che le aziende sono tenute a fare[57], senza una reale considerazione dei rischi complessi e in evoluzione posti dai sistemi autonomi di AI.

D'altronde, anticipando quanto si traccerà in sede di conclusioni, allorquando si guardi al contesto in cui nasce tale assetto regolativo, non si potrà non riconoscerne i limiti genetici che rendono oltremodo necessaria alla regolazione in materia di AI quella intelaiatura costituzionale di cui si è detto nel paragrafo precedente. Tale approccio nasce, infatti, in ambito economico ed è strettamente riconnesso al cosiddetto *Risk management* che, in adesione ad alcuni standard internazionali di riferimento, quali ad esempio la ISO 9001:2015 intende mappare determinati processi aziendali, al fine di migliorarne le qualità prestazionali[58].

Vi è tuttavia da dire che la legge europea non ritiene sufficiente l'approccio basato sul rischio, richiamando nel considerando 27 gli orientamenti etici per un'AI affidabile elaborati dall'AI HLEG indipendente nominato dalla Commissione nel 2019[59].

In tali orientamenti, l'AI HLEG ha elaborato sette principi etici non vincolanti per l'AI che sono intesi a contribuire a garantire che l'AI sia affidabile ed eticamente valida. I sette principi comprendono: intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e governance dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità.

In altri termini, fatti salvi i requisiti giuridicamente vincolanti del regolamento e di

[57] F. Paolucci, *Due process of Artificial Intelligence: a challenge for the protection of fundamental rights,* in G. Campus, et al. (ed.) *Digital Single Market and Artificial Intelligence*, Roma, 2024, 499 ss..

[58] Sul fronte delle specifiche tecniche, si veda il ruolo sempre più importante degli Enti di Normazione europea in fase di standardizzazione tecnica dei sistemi di AI (cfr. artt. 40; 43 AI Act) in cui alla valutazione tecnico – formale del rischio, si associa un vero e proprio *ethical assessment* posto a tutela dei diritti fondamentali.

[59] Si veda G. Finocchiaro, *Intelligenza artificiale. Quali regole*, Bologna, 2024 per una completa ricostruzione degli strumenti regolativi in materia di A.I.

qualsiasi altro diritto dell'Unione applicabile, tali orientamenti contribuiscono all'elaborazione di un'AI coerente, affidabile e antropocentrica, in linea con la Carta e con i valori su cui si fonda l'Unione. Ed è in questo contesto normativo che è stata concepita altresì la Convenzione europea sull'intelligenza artificiale adottata dal Consiglio d'Europa in cui si legge testualmente nella sua introduzione che si è inteso porre l'accento proprio su tali valori: *«… the Drafters also wanted to draw attention to human dignity and individual autonomy as foundational values and principles that are essential for the full realisation of human rights, democracy and the rule of law and that can also be adversely impacted by certain activities within the lifecycle of artificial intelligence systems».*

Tuttavia, l'etica s*oft,* è stato autorevolmente affermato, può funzionare solo in un contesto di legislazione adeguata, fiducia pubblica e responsabilità chiare in senso più ampio. L'accettazione pubblica e l'adozione di tecnologie digitali, compresa l'AI, avranno luogo soltanto se i benefici saranno percepiti come significativi ed equamente distribuiti, e i rischi come potenziali, ma prevenibili o minimizzabili[60]. È l'idea della democrazia deliberativa, basata su una situazione discorsiva ideale, libera da dominio e da disequilibri di potere tra i partecipanti al dialogo, che permetta di raggiungere un accordo sulla base dell'argomento migliore che dovrebbe fondare un "consenso" sulle tecniche di intelligenza artificiale[61]. Ciò apparrebbe desiderabile soprattutto se riferito alle tecniche di intelligenza artificiale ad alto rischio che, proprio per il loro grado di invasività nella sfera dell'umano, come detto in premessa, devono necessariamente essere connotate da un *ethical purpose* e da un obbligo di conformità ai valori fondamentali della convivenza civile, di rispetto alla dignità umana e dei diritti, eguaglianza e non discriminazione, quale uguale opportunità di accesso a queste possibilità tecnologiche, alle risorse del mondo digitale ricostruibili come beni comuni o come oggetto di un vero e proprio diritto sociale[62].

4. Conclusioni

In questa nuova dimensione ontica e deontologica, plasmata dalle forme dell'intelligenza artificiale, il limite della dignità umana, quale meta principio, si riannoda, dunque, al bene primario della integrità e della sicurezza personale riferendosi ad una connotazione strettamente mentale, legata all'interazione uomo - macchina ed agli effetti che queste modalità possono produrre sul comportamento umano, sul modo di considerare i sistemi agenti, in particolare, quando adottano fisicità antropomorfe, nonchè sulle influenze distorsive che si possono produrre anche sul piano emotivo soprattutto per le persone che si trovano in una condizione di debolezza e di vulnerabilità, quali i minori[63].

---

[60] L. Floridi, *Etica dell'intelligenza artificiale*, cit.

[61] J. Habermas, *Teoria dell'agire comunicativo. Vol. 1: Razionalità nell'azione e razionalizzazione sociale*, a cura di G.E. Rusconi, Bologna, 2022.

[62] T. E. Frosini, *Il costituzionalismo della società tecnologica*, in *Diritto dell'informazione e dell'informatica*, 4, 2020, 465 ss.

[63] Si veda il pensiero di A. d'Aloia in diversi lavori in materia, ed in specie: *Intelligenza artificiale, società*

È proprio con riferimento a tali principi che si auspica il superamento di un modello meramente organizzativo - formalista che possa garantire nello spazio economico europeo la diretta applicazione di uno *ius cogens* dell'intelligenza artificiale, che soprattutto sul piano dell'effettività della tutela, imponga validi ed efficaci strumenti di tutela dei diritti fondamentali potenzialmente a rischio.

Sulle prospettive *de iure condendo,* è di recente presentazione il disegno di legge in materia di A.I. che, sul fronte penale prevede un aumento della pena per i reati commessi mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, chiarisce il Governo, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, o quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa o aggravato le conseguenze del reato. Infine, attraverso apposita delega, il Governo dovrà prevedere: strumenti tesi ad inibire la diffusione e a rimuovere contenuti generati illecitamente anche con sistemi di intelligenza artificiale, supportati da un adeguato sistema di sanzioni; una o più autonome fattispecie di reato, punite a titolo di dolo o di colpa, nonché ulteriori fattispecie di reato, punite a titolo di dolo, dirette a tutelare specifici beni giuridici esposti a rischio di compromissione per effetto dell'utilizzazione di sistemi di intelligenza artificiale; una circostanza aggravante speciale per i delitti dolosi puniti con pena diversa dall'ergastolo nei quali l'impiego dei sistemi di intelligenza artificiale incida in termini di rilevante gravità sull'offesa; una revisione della normativa sostanziale e processuale vigente, anche a fini di razionalizzazione complessiva del sistema.

Se, dunque, il legislatore vira sullo strumento penale quale presidio effettivo nei confronti degli effetti potenzialmente distorsivi delle tecniche di intelligenza artificiale, si rende ancor più necessaria ed ineludibile l'elaborazione di una vigorosa dogmatica costituzionale in materia di intelligenza artificiale, esigenza richiamata all'inizio di tale contributo, poiché questa è oltremodo imposta da quell'altrettanta imprescindibile selezione dei beni giuridici primari che possono (e devono) fondare *ex necesse* la sanzione penale.

Nell'arcipelago complesso del digitale, il costituzionalista del *post-umanesimo*[64] è, dunque, chiamato ad un compito estremamente arduo, ossia, quello di esplorare l'orizzonte potenzialmente infinito delle possibilità offerte dall'intelligenza artificiale, in un dialogo costante con il linguaggio spurio della tecnica, con la saldezza della logica deontica dei principi – valori costituzionali e del super valore primario della dignità umana, quale bussola di orientamento nel magma accelerato del progresso.

algoritmica, dimensione giuridica. Lavori in corso, in *Quaderni costituzionali, Rivista italiana di diritto costituzionale*, 3, 2022.

[64] Sulle sfide che attendono il presente, laddove la tecnologia è costruita a somiglianza dell'essere umano, assumendo aspetti a volte salvifici, a volte inquietanti si veda M. Revelli, *Umano, Inumano, Postumano, Le sfide del presente,* Torino, 2020.

Intelligenza Artificiale e *deepfakes*: le nuove frontiere della disinformazione e i possibili rimedi giuridici*.

Maria Esmeralda Bucalo

Abstract

Partendo da alcune considerazioni su tecnologia e diritti, il lavoro si occupa delle nuove frontiere della disinformazione determinate dal sorgere e dall'evolversi dell'Intelligenza Artificiale, la quale, oltre che comportare nuove sfide per il costituzionalismo, riacuisce formule già esistenti di discriminazione. Attraverso l'esame di alcuni casi concreti occorsi sia in Europa sia negli Stati Uniti, avrà modo di evidenziare, infatti, come i *deepfake* siano in effetti i "successori" tecnologicamente evoluti delle *fake news* e le diverse risposte che predispongono gli ordinamenti fra le due sponde dell'Atlantico per fronteggiarli, che sembrano ricalcare quelle già predisposte per le forme già conosciute di disinformazione nell'era digitale.

Starting from some considerations on the combination of technology and rights, the work deals with the new frontiers of disinformation determined by the rise and evolution of Artificial Intelligence, which, in addition to posing new challenges for constitutionalism, sharpens already existing formulas of discrimination. Through the examination of some concrete cases that occurred both in Europe and in the United States, it will be able to highlight, in fact, how deepfakes are in fact the technologically advanced "successors" of fake news and the different responses that predispose the orders between the two shores of the Atlantic to face them, which seem to follow those already prepared for the already known forms of disinformation in the digital age.

Sommario

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

italiano sull'Intelligenza Artificiale – 8. Considerazioni finali.

Keywords

Intelligenza Artificiale – *deepfake* – disinformazione – giurisprudenza UE – normativa europea

1. Premessa

Le riflessioni oggetto del presente lavoro devono partire dalla considerazione preliminare per la quale tecnologia e diritti fondamentali costituiscono un binomio la cui somma algebrica è rilevante in diritto e non può non essere tenuto in considerazione. Infatti, partendo dalla definizione matematica di binomio[1] ed estendendola poi agli studi giuridici, può constatarsi che, sebbene tecnologia e diritti fondamentali siano ontologicamente due monomi fra loro non assimilabili, il corso della storia ci ha insegnato che essi sono necessariamente congiunti: la prima, infatti, è stato il fattore che ha contribuito, da un lato, alla interpretazione evolutiva di quelli già positivizzati nelle Costituzioni, nelle Dichiarazioni e nelle Carte di livello internazionale e sovranazionale, consentendo il loro adeguamento alle nuove esigenze dei tempi e, dall'altro, alla codificazione dei cosiddetti "nuovi diritti" o "diritti di nuova generazione" [2].

Ciò è ancor più vero nel XXI secolo, nel quale la rivoluzione tecnologica digitale (c.d. "quarta rivoluzione industriale)[3] ha cambiato radicalmente il modo di vivere di ciascuno, permeando in modo capillare anche l'ambiente giuridico.

La diffusione di *Internet* ha però seguito un percorso diverso rispetto alla diffusione degli strumenti tecnologici del passato, intanto perché sono stati soggetti privati (e

[1] Secondo la definizione matematica il binomio è un polinomio, ridotto in forma normale e composto dalla somma o dalla differenza di due monomi non simili.

[2] Per quanto concerne la libertà di espressione e manifestazione del pensiero, intorno alla quale ruotano le considerazioni che verranno rese qui appresso, si pensi all'invenzione della stampa che, oltre a contribuire allo sviluppo di un nuovo settore industriale, «ruppe il monopolio delle informazioni in capo a pochi privilegiati e consentì [...] l'accesso alla cultura a gruppi sempre più ampi» (così L. Torchia, *Lo Stato digitale,* Bologna, 2023, 35).

Fu così che, insieme al progredire della tecnologia e allo sviluppo della radio e della televisione come ulteriori mezzi di comunicazione, alla visione strettamente "individualista" della libertà di espressione, che determinava la necessità che lo Stato ed ogni apparato pubblico si astenesse da ogni azione che con essa potesse interferire, si sommò anche quella "funzionale e sociale", che determinava la necessità che i pubblici apparati intervenissero e regolassero il settore rendendolo fruibile a tutti i consociati e garantendo il pluralismo. In tema si veda L. Torchia, *Stato digitale,* cit., 17.

[3] La fortunata definizione è dovuta a K. Schwab, *La quarta rivoluzione industriale*, Milano, 2016. Si ritiene convenzionalmente che la prima rivoluzione industriale, fra la fine del XVIII e i primi decenni del XIX secolo, sia stata determinata dall'invenzione del motore a scoppio ed il conseguente aumento della produzione; la seconda, nel secolo successivo, dallo sviluppo dell'elettricità, dalla conseguente diffusione delle catene di montaggio e, dunque, delle produzioni di massa, che non richiedevano più specifiche competenze dei lavoratori; infine, la terza c.d. "informatica", che comincia negli anni '50 del secolo scorso con l'invenzione dei calcolatori elettronici, dalla diffusione della tecnologia digitale e di *Internet*, come mezzo che rende le informazioni accessibili a tutti anche da dispositivi mobili sempre più potenti e sempre più economici.

non pubblici) a organizzare e rendere disponibile a quante più persone i nuovi servizi; in secondo luogo, perché la capacità di incisione di questi nuovi mezzi di informazione e comunicazione nella vita personale e sociale assume dimensioni straordinarie, non coprendo più soltanto l'area dell'informazione, ma anche quella della elaborazione e della trasmissione delle culture[4].

In questa nuova rivoluzione tecnologica accade dunque ciò che in passato non si era mai verificato, e cioè che l'innovazione sia «al tempo stesso una caratteristica intrinseca del potere pubblico e un fenomeno la cui regolazione è centrale per i rapporti economici e sociali complessivamente intesi»[5].

La locuzione usata per riassumere e definire questa novità è "Stato Digitale", che presenta due nuove caratteristiche rispetto al passato. La prima è che l'attività pubblica nel suo complesso viene trasformata, quanto a mezzi e modalità di svolgimento, dall'uso delle nuove tecnologie, che ne determinano una riarticolazione e una riorganizzazione di funzioni e strutture.

La seconda è determinata dalla capacità di incisione dello sviluppo tecnologico sui rapporti sociali ed economici in modo tale da rendere sempre più obsolete e inidonee le regole vigenti. Da qui la necessità di una nuova regolazione pubblica volta ad aggiornare le discipline esistenti, con l'introduzione di nuove regole che si adeguino alla realtà attuale[6].

Le considerazioni che seguono hanno ad oggetto le nuove forme di manifestazione del pensiero e di espressione generate per mezzo della tecnologia, e in specie dell'Intelligenza Artificiale, che si diffondono attraverso la Rete su scala globale. Esse appaiono a prima vista l'evoluzione di quelle già sviluppatesi in "età digitale", grazie allo sviluppo dei *social media* e, più in generale, di tutte le piattaforme di condivisione.

Se così è, conseguentemente anche la disinformazione ha subito una analoga evoluzione grazie all'avanzamento tecnologico. Oggi, infatti, la diffusione di *fake news* viene sopravanzata dalla diffusione di *fake* generati dalla IA (i cc.dd. *deepfake*), che, grazie al maggiore impatto delle immagini e dei video artificialmente creati, hanno una capacità nociva e dannosa potenziata rispetto alle prime, spesso integrando fattispecie di reato e riacuendo discriminazioni.

Che i *deepfake* siano l'evoluzione delle *fake news* sarà reso evidente anche dall'analisi delle risposte e dei rimedi predisposti da ordinamenti diversi, che, come si avrà modo

[4] U. De Siervo, *Informazione, comunicazione globale e privacy*. Secondo K. Schwab, *La quarta rivoluzione industriale,* cit., 23, il *punctum crucis* che distingue la "quarta rivoluzione industriale" da quelle precedenti, è che essa non riguarda soltanto la diffusione di nuovi strumenti di comunicazione e di produzione, ma il fatto che essa determini anche mutamenti sociali, cambiando drasticamente il mondo in cui viviamo. Ciò si rileva anche dal fatto che il dato rilevante ai fini della sua individuazione non sia tanto la diffusione di nuovi strumenti tecnologici (si pensi alla diffusione dei calcolatori elettronici considerata convenzionalmente l'elemento determinante il sorgere della "terza rivoluzione industriale"), bensì la velocità dell'avanzamento tecnologico, la portata e l'intensità delle innovazioni, oltre che l'impatto prodotto sui sistemi aziendali, di produzione, ma anche sociali in generale.

[5] L. Torchia, *Lo Stato digitale,* cit.

[6] L. Torchia, *Prefazione*, in V. Bontempi (a cura di), *Lo Stato digitale nel Piano di Ripresa e Resilienza*, Roma, 2022, 11 ss., ma anche in *Lo Stato digitale,* cit., 22, spec. 18-19 l'A. spiega come l'aggettivo "digitale" si sommi oggi a quelli che hanno accompagnato l'evoluzione dello Stato, il quale certamente continua a svolgere tutte le funzioni assunte in precedenza.

di approfondire, ricalcano quelli già apprestati per le seconde. Essi possono ascriversi tutti al "costituzionalismo digitale", inteso come "nuova stagione del costituzionalismo", che tende ad «ampliare, a completare e a rafforzare gli strumenti del costituzionalismo tradizionale […] effetto diretto delle trasformazioni che la scienza e la tecnica hanno determinato nella sfera fisica, psichica e relazionale della persona umana»[7].
Si tratterebbe dunque di un "costituzionalismo globale" espansione del paradigma "costituzionale tradizionale" che, pur non volendo rompere con la tradizione e con il passato, guardano al futuro, optando per una rifondazione della democrazia costituzionale mediante l'introduzione di adeguate tecniche e funzioni di garanzia[8].
La risposta del diritto alle "rotture costituzionali"[9] e alle alterazioni dell'"equilibrio costituzionale" prodotte dalle tecnologie digitali, determinate dalla evoluzione tecnologica, dovrebbe essere reperita in un "processo di costituzionalizzazione dell'ambiente digitale" che consenta di bilanciarle, identificando nell'insieme di valori del costituzionalismo tradizionale le necessarie "contromisure"[10].

2. Problemi definitori dell'Intelligenza Artificiale

Fra le tecnologie sviluppate l'Intelligenza Artificiale è certamente quella maggiormente rilevante, essendo divenuta la forma più progredita di raccolta ed elaborazione dei dati, grazie ai meccanismi di *machine learning*, in grado di incidere profondamente sui diritti di ciascuno.
Essa da sempre ha stimolato grandi opere letterarie e cinematografiche che hanno contribuito a costruirne progressivamente il mito[11]. Menzionarle in questa sede ha un senso, perché contribuisce a ricordarci che la cultura di partenza sul tema, che in qualche modo ha formato le convinzioni (e i pregiudizi) di ciascuno su questa tecnologia, la descrive essenzialmente come fonte di grandi pericoli per l'umanità, capace di ribellarsi in modo autonomo ai suoi inventori, i quali ne perdono il controllo e possono

[7] E. Cheli, *Conclusioni*, in *Osservatorio sulle fonti*, 2, 2021, 955-956.
Si veda anche P. Costanzo, *Il fattore tecnologico e le sue conseguenze*, relazione tenuta al convegno annuale della Associazione Italiana dei Costituzionalisti, svoltosi a Salerno 23-24 novembre 2012, 28, che parla di «costituzionalismo tecnologico»; G. Azzariti, *Internet e Costituzione*, in *costituzionalismo.it*, 2, 2011, e G. De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorythmic Society,* Cambridge, 2022.

[8] L. Ferrajoli, *Costituzionalismo oltre lo Stato*, Modena, 2017, 44 ss. L'A. più recentemente ha sviluppato le stesse tesi in *Il futuro del costituzionalismo*, in *costituzionalismo.it*, 2, 2022, 182 ss. Analogamente L. Antonini, *Globalizzazione e nuove sfide del costituzionalismo*, in *Diritto pubblico*, 2, 2019, 319 ss.

[9] F. Balaguer Callejon, *La Constitucion de l'algoritmo*, Zaragoza, 2023, 16-17, il quale afferma che la «Costituzione analogica» regola «un mondo che in parte non esiste più o è divenuto socialmente irrilevante» ed è necessario invece «analizzare la realtà digitale dal punto di vista delle rotture che essa sta generando e che hanno una dimensione costituzionale», al fine di «proporre soluzioni che permettano di mitigare tali rotture e facilitino una risposta costituzionale».

[10] E. Celeste, *Digital Constitutionalism: a new systematic theorization*, in *International Review of Law*, 1, 2019, 88, 93 e 99.

[11] Fra le prime va menzionata la produzione di Asimov datata anni 30 del secolo passato, mentre fra le seconde capolavori come *2001: Odissea nello spazio* (di Kubrick del 1968) *Blade Runner, Matrix* e più di recente *L'uomo bicentenario* e *Her.*

rimediarvi solo staccando la spina[12].

Come è stato rilevato, non si può non tenere in considerazione come tale portato culturale abbia influenzato (e influenzi a tutt'oggi) anche l'approccio giuridico, e scientifico in generale, a questa tecnologia[13], tanto che il suo sviluppo è stato negli anni molto ondivago, alternando a periodi di grandi interesse e investimenti, periodi di disaffezione per l'argomento (denominati comunemente *"AI Winter"*)[14].

L'indubbia complessità del tema deriva, non solo dalla difficile caratterizzazione delle diverse tipologie di funzionamento dell'IA, ma anche, in via preliminare, dal punto di vista definitorio[15].

Nel ricordare che il primo studio scientifico sulla IA fu firmato dal matematico Alan Mathison Turing e risale alla prima metà del XX secolo[16] e che ad esso fece seguito il "*Dartmouth Summer Project Research on Artificial Intelligence*"[17], che per la prima volta configurò l'Intelligenza Artificiale come autonoma disciplina scientifica[18], è bene rammentare anche il metodo, invero ancora attuale, ivi a tal fine adottato.

Turing, infatti, piuttosto che definire cosa fosse l'intelligenza, cosa invero assai difficile, preferiva confrontare i risultati di un processo: se il processo era qualificato intelligente quando svolto da un essere umano, allora il raggiungimento di uguali risultati attraverso un processo svolto da una macchina determina che anche quest'ultimo poteva essere definito "intelligente"[19].

---

[12] G. Finocchiaro, *Intelligenza Artificiale. Quali regole?,* Bologna, 2024, 16.

[13] G. Finocchiaro, ivi, 17 ritiene che tale portato culturale influenzi anche gli aspetti giuridici strettamente tecnici, poiché non si può dimenticare che «coloro che interpretano o scrivono le regole sono inevitabilmente condizionati dalla cultura di cui sono portatori».

[14] G.F. Italiano, *Intelligenza Artificiale: passato, presente, futuro,* in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 209 ricostruisce un primo periodo (1974-1980), nel quale si registra la carenza di attenzione introno agli studi scientifici sull'argomento sono seguiti alla diffusione di due report (rispettivamente del 1966 dell'*Automatic Language Processing Advisory Committe* del governo statunitense e quello denominato *Lighthill* del 1973 del governo inglese), che ritennero improbabile nel breve periodo lo sviluppo di tale tecnologia, tagliando dunque i relativi finanziamenti; mentre il secondo *"AI Winter"* andrebbe dal 1987 al 1993. Sebbene ancora nei primi anni del XXI secolo il tema non godesse di grande attenzione, oggi le ricerche sull'IA vivono la loro *"AI Spring"* (o *"AI Boom")* registrando i più alti livelli di interesse e finanziamento nella storia.

[15] Sulla difficoltà definitoria associata all'IA, M.U. Scherer, *Regulating Artificial Intelligence Systems: risks, challanges competencies, and strategies,* in *Harvard Journal of Law & Technology,* 2, 2016, 359, nonché C. Casonato, *Intelligenza Artificiale e diritto costituzionale: prime considerazioni,* in *Diritto pubblico comparato ed europeo,* numero speciale, 2019, 102-103.

[16] Ci si riferisce in particolare agli studi di A.M. Turing, *Computing Machinery and Intelligence*, in *Mind*, 236, 1950, 433 ss.

[17] Proposta da J. Mccarthy – M.L. Minsky – N. Rochester – C.E. Shannon, *A proposal for the Dartmouth summer research project on artificial intelligence*, 31agosto 1955, 1.

[18] Alla conferenza parteciparono anche altri sei studiosi: Ray Solomonoff, Oliver Selfridge, Trenchard More, Arthur Samuel, Allen Newell e Herbert Simon. Fra questi in particolare, Newell e Simon presentarono il *Logic Theorist*, il primo programma esplicitamente progettato per imitare le capacità di *problem solving* degli esseri umani.

[19] A.M. Turing, *Computing Machinery and Intelligence,* cit., 433. Si tratta dell'*Imitation Game* di A.M. Turing, *Computing Machinery and Intelligence*, cit., 433, ideato per determinare se una macchina sia in grado di effettuare collegamenti, concatenare idee ed infine esprimerle. Con estrema esemplificazione può dirsi che secondo l'A. l'intelligenza artificiale è la scienza di far fare ai computer cose che richiedono intelligenza quando vengono compiute da esseri umani. Dunque, chiedersi se le macchine possono

A dimostrare l'importanza e l'interesse trasversale che suscita il tema, è bene notare che l'"approccio controfattuale", nato nell'area delle c.d. "scienze dure", è stato ripreso recentemente e sviluppato anche in ambito umanistico e filosofico da Luciano Floridi che ribadisce che l'IA non ha nulla a che fare con l'intelligenza, poiché «separa la capacità di risolvere un problema o di portare a termine un compito con successo dalla esigenza di essere intelligenti per farlo»[20].

Lo stesso A. ritiene che di IA non esista una definizione univoca come per molte delle «cose importanti della vita […] (che) spesso non sono affatto definibili», ma che riconosciamo quando le vediamo. Di conseguenza è possibile ritenere che «IA non è un termine scientifico, […] ma un'espressione generica […] una scorciatoia, usata per riferirsi approssimativamente a diverse discipline, servizi, prodotti tecnoscientifici talora solo genericamente correlati»[21].

Riprendendo quanto sopra rilevato sul retaggio culturale intorno alla IA, è possibile allora ritenere, come lo stesso fa Floridi, che della IA esistano "due anime", una "ingegneristica" (altrimenti detta "riproduttiva") e l'altra "cognitiva" (detta anche "produttiva"). La prima interessata alla riproduzione di comportamenti umani definiti intelligenti (e che è quella di cui scientificamente ci si occupa), l'altra come settore della scienza cognitiva interessata alla produzione di intelligenza, che attualmente resta una idea fantascientifica[22].

La mancanza di una piena autonomia definitoria è evidente anche nell'ambito più strettamente giuridico, come dimostrato anche da recenti atti normativi (e para-normativi).

Nella Risoluzione del Parlamento Europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, l'IA sembra essere intesa quale elemento strumentale allo sviluppo di altre tecnologie, essendo maggiormente incentrata sul concetto di "robot autonomo intelligente" e non come fenomeno a sé stante e non necessariamente legato ad una componente *hardware*[23].

Più utile è invece quella resa dal Gruppo di Esperti sull'Intelligenza Artificiale nominato dalla Commissione Europea nel 2019, per la quale «I sistemi di Intelligenza Artificiale (AI) sono sistemi software (ed eventualmente anche hardware) progettati da esseri umani che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il loro ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulla conoscenza, o l'elaborazione

pensare era per Touring una domanda «troppo insensata per meritare di essere discussa». Sul punto si veda anche G. Finocchiaro, *Intelligenza Artificiale*, cit., 22.

[20] L. Floridi, *Etica dell'Intelligenza Artificiale. Sviluppi, opportunità, sfide*, Milano, 2022, 41, il quale ritiene anche che «l'IA non concerne la capacità di riprodurre l'intelligenza, ma in realtà la capacità di farne a meno».

[21] Ivi, 42.

[22] Ivi, 48-50.

[23] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2013INL). Specificatamente si veda l'allegato a detta Risoluzione ove si rende una definizione di *robot* autonomo intelligente e non di IA in senso autonomo dalla robotica. Sottolineano le criticità di tale definizione C. Cath – S. Wachter – B. Mittelstadt – M. Taddeo – L. Floridi, *Artificial Intelligence and the "Good Society": the US, EU, and UK approach*, in *Science and Engineering Ethics*, 2, 2018, 514-515.

delle informazioni, derivata da questi dati e decidere le migliori azioni da intraprendere per raggiungere l'obiettivo prefissato. I sistemi di intelligenza artificiale possono utilizzare regole simboliche o apprendere un modello numerico e possono anche adattare il proprio comportamento analizzando il modo in cui l'ambiente è influenzato dalle loro azioni precedenti»[24].

La correttezza della definizione citata appare peraltro confermata dall'*AI Act* che al suo art. 3 definisce l'IA come «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»[25].

Entrambe le definizioni hanno il pregio di non antropomorfizzare l'IA ed evitano di riproporre il confronto uomo-macchina, che era presente negli studi sulla Intelligenza Artificiale fin dai suoi albori, non associando ai sistemi artificiali né il concetto di intelligenza umana né altre facoltà tipicamente legate alla sfera biologica[26].

Inoltre, la stessa consente anche di tracciare una distinzione fra ciò che ad oggi può essere inteso verosimilmente rientrare nel concetto di IA e ciò che, invece, rimane distante dalla realtà. In particolare, il Gruppo di Esperti fa una netta distinzione tra "IA generale" (o IA forte) e "IA ristretta" (o IA debole). Quest'ultima tipologia rimane circoscritta ad una forma di abilità funzionale per lo svolgimento di compiti specifici[27], mentre, l'IA generale descrive un sistema dotato di estrema versatilità e pertanto capace di svolgere qualsiasi attività eseguibile da parte di un essere umano.

Sarebbe, dunque, la "IA ristretta" a rappresentare la tipologia dei sistemi artificiali ad

---

[24] High-Level Expert Group on Artificial Intelligence, *Una definizione di IA: principali capacità e discipline*, Bruxelles, 8 aprile 2019, 6. La definizione consta anche di una seconda parte che considera la IA come una disciplina scientifica affermando che «In quanto disciplina scientifica, l'intelligenza artificiale comprende diversi approcci e tecniche, come l'apprendimento automatico (di cui il deep learning e l'apprendimento di rinforzo sono esempi specifici), il ragionamento automatico (che include pianificazione, programmazione, rappresentazione e ragionamento della conoscenza, ricerca e ottimizzazione) e la robotica (che comprende il controllo, la percezione, i sensori e gli attuatori, nonché l'integrazione di tutte le altre tecniche nei sistemi ciberfisici).» La definizione perfeziona quella precedentemente proposta dalla Commissione europea, *Comunicazione su L'Intelligenza artificiale per l'Europa*, Bruxelles, 25.4.2018, COM(2018) 237 final, 1 « L'intelligenza artificiale (AI) si riferisce a sistemi che mostrano un comportamento intelligente analizzando il loro ambiente e intraprendendo azioni – con un certo grado di autonomia – per raggiungere obiettivi specifici. I sistemi basati sull'intelligenza artificiale possono essere puramente basati su software, agendo nel mondo virtuale (ad esempio assistenti vocali, software di analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale) oppure l'intelligenza artificiale può essere incorporata in dispositivi hardware (ad esempio robot avanzati, automobili autonome, droni o applicazioni Internet of Things).»

[25] Sull'*AI Act* si veda *infra* § 7.2.

[26] Così R. Cucchiara, *Intelligenza Artificiale e Italia. Sfide e opportunità*, in 2, *Gnosis*, 2019, 48-49. Analogamente, L. Floridi, *What the near future of Artificial Intelligence cloud be*, in *Philosophy & Technology*, 32, 2019, 2-3, non fa riferimento al concetto di intelligenza quanto piuttosto a quello di *agency*, intesa come abilità d'azione, tanto da definire l'IA quale «reservoir of smart agency on tap». R. Cingolani, *Il corpo e la mente. Robot e uomini nel futuro dell'Intelligenza Artificiale*, in 2, *Gnosis*, 2019, 75-76 riassume efficacemente la distinzione fra uomo e IA affermando che «il robot segue le leggi dell'elettricità, il corpo umano quelle della biochimica». Sulla necessità di non antropomorfizzare l'IA anche G. Finocchiaro, *La regolazione dell'Intelligenza artificiale,* in *Rivista trimestrale di diritto pubblico,* 4, 2022, 1087.

[27] R. Cingolani, *L'altra specie. Otto domande su noi e loro*, Bologna, 2019, 105 ss.

oggi effettivamente implementati ed in uso, mentre la "IA generale" l'obiettivo, definito "utopico"[28], che suscita vivaci dibattiti, ma, in modo rassicurante per tutti, non trova applicazioni concrete[29].

Con molta semplificazione, può dirsi quindi che l'Intelligenza Artificiale non opera secondo un ragionamento logico, ma è un *software* che si avvale di un'impostazione *data-driven,* il quale, attraverso l'elaborazione dei dati, porta il sistema artificiale a sviluppare e seguire un proprio modello matematico per svolgere l'operazione che gli è stata assegnata.

Posta tale definizione, il Gruppo di Esperti ne propone una bipartizione che individua due "macroaree" distinte in base alla capacità di apprendere e ricalibrare la propria attività in relazione ai mutamenti intervenuti nell'ambiente in cui la macchina opera.

Una prima categoria di sistemi di IA si limita a riprodurre in maniera automatizzata il meccanismo in essi contenuto, risultando capaci di giungere all'obiettivo assegnatoli a partire dai dati raccolti in ingresso e seguendo stabilmente, volta dopo volta, il processo decisionale e di elaborazione-ragionamento descritto all'interno del loro codice (il c.d. *data-set* individuato dal programmatore e da lui inserito nel sistema di IA). In questi casi, dunque, la macchina esegue processi automatizzati lineari, caratterizzati da meccanismi di *input-output* e da una forte corrispondenza tra l'impulso iniziale e l'esito del processo.

Una seconda categoria più complessa costituita dai sistemi di IA che a quanto sopra descritto aggiungono una autonoma "capacità di apprendimento", cosicché, attraverso l'interazione con il contesto circostante e l'assimilazione di nuove informazioni, risultano in grado di cambiare la propria strategia comportamentale (c.d. sistemi *machine learning*).

Di conseguenza, questi sistemi non operano solo attraverso procedimenti lineari (*input-output*), ma, a prescindere dall'input immesso in avvio, sono in grado di tenere in considerazione sia l'ambiente circostante sia l' "esperienza pregressa" costituita dagli *output* precedentemente emessi. In tal modo acquisiscono una certa autonomia dall'intervento umano del programmatore e ricalibrano il proprio "comportamento" sulla base dei riscontri avuti dalle passate interazioni con il contesto di riferimento.

Fra queste si distinguono i modelli più semplici e quelle di *deep learning*. I modelli più semplici si organizzano su tre livelli: il livello di *input* dei dati, il livello nascosto (*hidden layer*) destinato all'elaborazione delle informazioni e, da ultimo, il livello di *output* che produce l'esito del processo algoritmico.

I secondi, invece, risultano più complessi e maggiormente articolati, e si caratterizzano per essere composti da più livelli, ciascuno dei quali riceve *input* dallo strato precedente e alimenta con il proprio *output* lo strato successivo. Sono dunque chiamati sistemi di *deep learning,* perché sono in grado di completare più sofisticati processi di addestramento o di analisi di dati, appunto con "maggiore profondità".

Se quanto appena rilevato è certamente utile ai fini della definizione e della compren-

[28] High-Level Expert Group on Artificial Intelligence, *Una definizione di IA: principali capacità e discipline*, cit., 5-6.

[29] Commission nationale informatique & libertes, *How can human keep the upper hand? The ethical mat-ters raised by algorithms and artificial intelligence*, December 2017, 19.

sione di ciò che è Intelligenza Artificiale, delle sue diverse tipologie e dei suoi meccanismi di funzionamento, ritornando all'ambito giuridico che ci compete, ciò che risulta ancora troppo poco indagato (e regolato) sono le modalità attraverso le quali i dati vengono elaborati e immessi in tali sistemi, nonché la ricostruzione del procedimento attraverso il quale gli stessi sistemi di IA raggiungono determinati risultati, soprattutto laddove si faccia riferimento ai citati sistemi di *deep learning*.

3. Intelligenza Artificiale e nuove forme di discriminazione e disinformazione: i *deepfake*

La crescente penetrazione dell'IA in ogni aspetto del nostro vivere quotidiano e l'oscurità delle regole sulla base delle quali questa nuova tecnologia elabora i dati pongono necessariamente degli interrogativi, ai quali il diritto costituzionale ha il compito di rispondere, in modo da trarne tutti i possibili vantaggi e benefici ed evitando che i diritti della persona subiscano una ingiustificata compressione.
La capacità di incisione di tale tecnologia sui diritti fondamentali è l'oggetto delle riflessioni che seguono e che si occuperanno in particolare del diritto di informazione e della libertà di manifestazione del pensiero, indagando anche i profondi pregiudizi che l'uso dell'Intelligenza Artificiale comporta per l'individuo e la sua personalità, ivi compresi gli aspetti più intimi e delicati della stessa, come quelli attinenti alla sessualità.
Su questo versante, sempre preliminarmente, si può fare riferimento, per esempio, ai *sex robots* definibili come «una entità artificiale con forma umanoide, comportamenti quasi umani, un certo grado di intelligenza, usati per scopi sessuali»[30]. Come è evidente l'uso di queste macchine pone questioni profonde e intime, che riguardano i caratteri connotativi dell'essere umano che, sul versante giuridico, coinvolgono il principio di eguaglianza di genere e di non discriminazione[31].
In tema di *sex robots,* anche al fine di indagare i risvolti disinformativi che può avere l'uso della IA nella generazione di immagini, va citato il caso della diffusione *on line* della notizia, accompagnata dalla relativa foto generata dalla IA, per la quale Elon Musk sarebbe stato sul punto di presentare la sua fidanzata *robots*. La notizia poi rivelatasi falsa[32] era esplosa sui *social networks*, senza però essere mai stata ufficialmente smentita dallo stesso Musk o dalle sue aziende, le quali invero lavorano già da tempo alla realizzazione di *robot* umanoidi progettati però per svolgere compiti fisici e non per

[30] R. Halwani nella recensione a J. Danaher – N. Macarthur (eds.), *Robot Sex: Social and Ethical Implications*, Cambridge, 2017 ospitata in *Bioethics*, 32, 2018, 639.

[31] C. Nardocci, *Intelligenza artificiale e discriminazione,* in *La Rivista Gruppo di Pisa,* 3, 2021, 9.
In riferimento alla questione di genere, inoltre, è stata osservata una azione definita come *robots gendering,* ossia quella volta ad avere un forte impatto sull'attività e il comportamento delle persone attraverso la manipolazione della voce e delle caratteristiche estetiche del *robot*. Gli studi dimostrano, infatti, come siano prevalentemente i maschi a considerare socialmente utili i *sexbots*, caratterizzati in senso per lo più femminile, e come evidentemente ciò conduca a stereotipi di genere già fortemente presenti in molte società. Si veda T. Nomura, *Robots and Gender*, in *Gender and the Genome*, 1, 2017, 18; M. Scheutz – T. Arnold, *Are we ready for sex robots?*, in *The Eleventh ACM/IEEE International Conference on human robot interaction*, 07 March 2016, 351.

[32] Si veda l'articolo pubblicato su *Open* il 30 maggio 2023.

"funzioni sociali" o "emotive"[33].

Se forse i *sexrobots* ci sembrano ancora una realtà eccessivamente lontana, basti pensare che le discriminazioni che il loro utilizzo può comportare hanno il loro prototipo negli "assistenti vocali" che utilizziamo quotidianamente (Siri o Alexa). Progettati per essere in ogni momento a completa disposizione del loro "padrone", difficilmente vengono realizzati con "sembianze" maschili, presentando, al contrario, il più delle volte, nomi e voci di donna, a cui viene affidato il compito di rivolgersi in maniera accondiscendente nei confronti dell'interlocutore e di esaudire qualsiasi richiesta gli venga fatta, anche laddove quest'ultima risulti sgradevole, offensiva o inopportuna.

Così una semplice scelta progettuale di questo tipo alla base dello strumento tecnologico perpetua e rafforza gli stereotipi discriminatori esistenti nei confronti del genere femminile, confinando la figura della donna ad un ruolo di subalternità e di assoggettamento, respingendo l'idea che la stessa possa occupare posizioni diverse[34].

A ciò possiamo aggiungere ulteriori utilizzi dell'IA che, oltre che riacuire la discriminazione fondata sul genere, possono produrne anche in ragione dell'origine etnica e del colore della pelle. Si fa riferimento, per esempio, all'implementazione sui dispositivi mobili e sui computer dei sistemi *facial recognition*, che soprattutto in occidente sono sviluppati per lo più sulla base di data set contenenti immagini di uomini e donne bianchi, con una conseguente sottorappresentazione di individui di diversa origine etnica e la possibilità di pervenire a risultai inesatti[35].

Le discriminazioni di genere ed etniche, già presenti nel passato, riemergono quindi in senso fortemente accentuato in quanto rinnovate dall'uso dello strumento tecnologico e dall'enorme quantitativo di dati, tanto che da più parti viene rilevato come in generale il diritto costituzionale e pubblico non risultino pienamente in grado di tutelare l'individuo dalle disparità di trattamento che possono derivare dall'utilizzo di sistemi di Intelligenza Artificiale[36].

La capacità discriminatoria della IA e la sua mancata neutralità[37] dipendono da una molteplicità di ragioni che attengono per lo più alla costruzione del *data-set*[38], cioè dall'introduzione di quell'insieme di dati di cui la macchina dispone per compiere le

[33] Si veda il video riportato dal *Corriere delle sera*, 11 ottobre 2024.

[34] Sul punto si veda N. Loideain – R. Adams, *From Alexa to Siri and the GDPR: The gendering of Virtual Personal Assis- tants and the role of Data Protection Impact Assessment*, in *Computer Law & Security Review*, 2020, 36.

[35] Si legga in tal senso European union agency for Fundamental rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, November 2019, 27.

[36] Si veda per esempio F.Z. Borgesius (eds.), *Discrimination, artificial intelligence, and algorithmic decision-making*, Council of Europe, Strasbourg, 2018, 18 ss. e L. Giacomelli, *Big brother is «gendering» you. Il diritto antidiscriminatorio alla prova dell'intelligenza artificiale: quale tutela per il corpo digitale*?, in *Biolaw Journal – Rivista di Biodiritto*, 2, 2019, 278 ss. Analogamente esprimeva la stessa opinione in tema di diritto del lavoro L. Peruzzi, *Il diritto antidiscriminatorio al test dell'Intelligenza Artificiale,* in *Labour & Law Issue,* 1, 2021, 50 ss.

[37] M.V. Craiut – I. Iancu, *Is technology gender neutral? A systematic literature review on gender stereoptypes attached to artificial intelligence,* in *Human Technology,* 2022, 18(3), 297-315 e M. Airoldi – D. Gambetta, *Sul mito della neutralità algoritmica*, in *The Lab's Quarterly*, 4, 2018, 25 ss. Analogamente M. D'Amico – C. Nardocci, *Intelligenza artificiale e discriminazione di genere: rischi e possibili soluzioni,* in G. Cerrina Feroni – C. Fontana – E.C. Raffiotta (a cura di), *AI Anthology,* cit., 251; M. D'Amico, *Una parità ambigua,* Milano, 314 e 319 e S. Barocas – A.D. Selbst, *Big Data Disparate Impact,* in *California law Review,* 2016, 671 ss.

[38] K. Crawford, *The Hidden Biases in Big Data,* in *Harvard Business review,* 2013.

scelte per le quali viene programmata[39]; dalla associazione tra i dati[40]; nonché da possibili casi di *proxy discrimination,* che si verificano quando un dato formalmente neutro viene elaborato dal sistema di apprendimento automatico in modo da realizzare una discriminazione in via mediata senza che l'utilizzatore ne sia consapevole[41]. La novità determinata dall'avvento di questa nuova tecnologia è legata alla circostanza che in questo caso il carattere *proxy* potrebbe essere individuato autonomamente dal sistema di apprendimento automatico, senza che l'utilizzatore ne sia consapevole.

In casi più gravi, è possibile che la macchina sia stata volutamente programmata per ottenere risultati discriminatori, poiché è proprio il programmatore umano a rendere la macchina uno strumento di discriminazione[42]. È evidente che queste ultime forme di discriminazione siano più facilmente e immediatamente individuabili, mentre tendono a sfuggire alle successive verifiche quelle inintenzionali, che originano dagli stessi algoritmi.

A queste discriminazioni di genere operate dall'Intelligenza Artificiale, per lo più dipendenti dall'uomo che agisce nella programmazione sulla base di pregiudizi legati alla struttura non paritaria della società, si deve aggiungere poi la marginalizzazione femminile che vede le donne estromesse da settori scientifici e disciplinari nevralgici per lo sviluppo dell'Intelligenza Artificiale che ancora sono "monopolio maschile"[43].

Se questi sono i dati di partenza, a rendere ancor più evidente la gravità del fenomeno dell'utilizzo non corretto della IA e come tale utilizzo non corretto possa incidere sulla libertà di espressione, anche in senso discriminatorio, sono i cosiddetti *deepfake.*

Il termine è un neologismo nato dall'incrocio tra la locuzione *deep learning* e *fake* e si riferisce a contenuti multimediali, quali immagini, video, audio e testo, falsi che sono generati o manipolati utilizzando algoritmi appunto di *deep learning*: l'intento è quello di indurre colui che li osserva a percepirli come una rappresentazione fedele della realtà[44].

---

[39] In pratica, se ad una macchina si forniscono fin dall'origine dati errati, falsati o incompleti, la macchina risponderà analogamente in modo errato, falsato o incompleto. In questo caso, i *data-set* possono anche essere costruiti sulla base di pregiudizi e discriminazioni implicite, presenti cioè nella mente e/o nella cultura del programmatore.

[40] I dati forniti possono essere corretti, ma, soprattutto per le *machine learning* che operano autonomamente, la loro associazione può essere errata e portare a risultati e scelte discriminatorie "in uscita", anche non previsti o non voluti in sede di programmazione.

[41] Si veda in tema A.E.R. Prince – D. Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data,* in *Iowa Law revin,* 2020, 1257 ss.

Tali forme di discriminazione sono, invero, una pratica risalente cui si faceva ricorso ben prima della nascita dei sistemi di Intelligenza Artificiale. Si ricordi per esempio che, nella metà del 1900, per non concedere prestiti ai neri alcune banche utilizzarono l'indicazione dei codici postali o i confini dei quartieri al fine di escludere i prestiti a quartieri abitati per lo più da afroamericani, invece di operare una discriminazione diretta sulla base della razza. Ne parla F.Z. Borgesius, *Discrimination, Artificial Intelligence and Algorithmic Decision-Making,* Council of Europe, Strasbourg, 2018, 13-14.

[42] In tema si veda A. Venanzoni, *La valle del perturbante: il costituzionalismo alla prova delle intelligenze artificiali e della robotica*, in *Politica del diritto*, 2019, 2, 237-238, nonché P. Zuddas, *Intelligenza Artificiale,* in *Liber amicorum per Pasquale Costanzo*, 16 marzo 2020, 7 e G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del diritto*, 2, 2019, 208

[43] M. D'Amico – C. Nardocci, *Intelligenza artificiale,* cit., 256-258.

[44] Sulla nascita di tale fenomeno, sul suo intersecare la tematica della libertà di informazione, nonché per un esame della risposta normativa europea attraverso anche lo *Strengthened Code of Practice on Disinformation* si veda M. Cazzaniga, *Una nuova tecnica (anche) per veicolare disiformazione: le risposte europee ai*

La loro nascita è fissata convenzionalmente alla fine del 2017, quando un anonimo gruppo con lo pseudonimo *Deepfakes* pubblica i primi video falsi di natura pornografica su un *social* molto popolare chiamato *Reddit*, facendo uso dell'applicazione *FakeApp*: si trattava di immagini e video di star di Hollywood, realizzati a loro insaputa[45].
Dopo questo evento, nonostante la circolazione di *deepfake* pornografici sia stata proibita e bloccata tramite la rimozione degli stessi sulle piattaforme *social*, la creazione e divulgazione di *deepfake* è diventata inarrestabile[46].
L'ultimo caso eclatante che ha coinvolto un personaggio famoso risale peraltro solo a gennaio 2024, quando furono diffuse in modo virale sulla piattaforma *social X* immagini false, create con IA, della popstar Taylor Swift in atteggiamenti provocanti e atti sessuali[47]. Solo pochi giorni più tardi *X* metteva in atto una forma di censura inedita, rendendo inattive le ricerche col nome dell'artista. Il caso ha riaperto il dibattito in USA sulla necessità di disposizioni legislative per arginare i *fake*, sul modello del DSA europeo.
I *deepfake* vengono impiegati in diversi settori, come il cinema, la medicina, l'arte, le comunicazioni digitali, l'intrattenimento, per scopi commerciali (*e-commerce* e moda) e costituiscono la naturale evoluzione di altri metodi di contraffazione di dati sintetici, come la *Computer Graphica* (in grado di contraffare immagini e video digitali in 2D e 3D) e *Auto-tune* (primo *software* in grado di manipolare audio in modo autonomo).
Secondo il rapporto 2023 dell'Istituto Europeo per le norme delle Telecomunicazioni (ETSI) intitolato *"Securing Artificial Intelligence (SAI); Automated Manipulation of Multimedia Identity Representations*" «il rapido progresso della tecnologia informatica negli ultimi decenni ha reso sempre più semplice anche la manipolazione di foto, file audio e video, (perché) le tecniche di intelligenza artificiale consentono di automatizzare manipolazioni che in precedenza richiedevano una notevole quantità di lavoro manuale.»[48]
Dunque, a differenza del loro esordio, nel quale i *deepfake* ritraevano principalmente personaggi famosi, adesso invece chiunque può diventare vittima di tali contenuti. Ciò evidentemente determina «rischi sostanziali in vari contesti che vanno dalla diffamazione personale e alla apertura di conti bancari utilizzando false identità (attraverso attacchi alle procedure di autenticazione biometrica) fino alle campagne per influenzare l'opinione pubblica»[49].
Su quest'ultimo tema si ricordi da ultimo che a gennaio 2024, a poche ore dalle primarie statunitensi nel New Hampshire molti cittadini hanno ricevuto una *robocall* falsa, nella quale una voce del tutto uguale a quella del presidente Biden (evidentemente

deepfakes, in questa *Rivista*, 1, 2023, 170 ss.

45 Sul primo caso di deepfake, S. Maddocks, *'A Deepfake Porn Plot Intended to Silence Me': exploring continuities between pornographic and 'political' deepfakes*, in *Porn Studies*, 7, 2020, 415 ss.

46 Sul caso Taylor Swift, S. Ruiz Lichter, *Why the Taylor Swift AI Scandal is Pushing Lawmakers to Address Pornographic Deepfakes,* in *The National Law Review,* 22 aprile 2024. Sulla normativa europea *infra* § 7.

47 Le visualizzazioni di uno dei deepfake, di cui la cantante era vittima, sono state 45 milioni, con almeno 24 mila condivisioni e incalcolabili apprezzamenti degli utenti. "*Taylor Swift Ai*" è diventato presto un termine di ricerca in tendenza sulla piattaforma, con le immagini rimaste online per ore.

48 *Securing Artificial Intelligence (SAI); Automated Manipulation of Multimedia Identity Representations*, Istituto Europeo per le norme delle Telecomunicazioni (ETSI), rapporto 2023, 11.

49 *Securing Artificial Intelligence (SAI); Automated Manipulation of Multimedia Identity Representations*", cit., 10.

generata con IA), invitava a non votare e a conservare il proprio voto per le elezioni di novembre[50].

Ovviamente tutto ciò getta delle ombre oscure e preoccupanti sulla capacità manipolativa anche del consenso elettorale da parte di coloro che sono in grado di creare *deepfake*[51].

D'altro canto e in senso più specifico, i dati diffusi dall'Autorità Garante per protezione dei dati personali italiana, nonché filoni di ricerca recenti, evidenziano in modo preoccupante che oltre il 90% dei video *deepfake* si configurano come materiale a contenuto pornografico e che nella quasi totalità dei casi (98%) essi hanno ad oggetto donne[52].

Tale evoluzione deteriore dei *deepfake* è denominata "*deepfake pornography*", locuzione che fa riferimento all'utilizzo di tecniche generative per l'alterazione di immagini e video con contenuto pornografico.

Le vittime del contenuto in questione vengono "spogliate" artificialmente ed appaiono in atteggiamenti sessualmente espliciti, che in realtà sono a loro estranei. Poiché le immagini sono modificate artificialmente con la tecnica dello *face-swap* e, dunque, i protagonisti non sono effettivamente coinvolti nell'atto sessualmente esplicito, la creazione e la successiva divulgazione di tali contenuti comportano una lesione della loro dignità e della loro privacy, in quanto collocati forzatamente in un contesto a cui non appartengono, e conseguenzialmente l'insorgere di numerose fattispecie penalmente rilevanti, fra cui il furto di identità[53].

---

[50] Analogamente qualche giorno dopo, un video diffuso su *Facebook*, manipolato anch'esso attraverso l'IA, etichettava lo stesso presidente come "pedofilo schifo", mentre invece la ragazza baciata era la nipote. Si veda *Deepfake alle primarie USA. Clonata la voce del presidente Biden. Telefonata falsa finalizzata a invitare gli elettori a disertare il voto,* in *ansa.it,* 29 gennaio 2024.

[51] Si veda *Biden, un video manipolato sui social che lo accusa di pedofilia. Meta, un'etichetta contro i deepfake*, in *corriere.it,* 6 febbraio 2024.
Quanto alla formazione dell'opinione pubblica manipolata da *fake news* che circolano online soprattutto in periodi di elettorale si permetta di rinviare a M.E. Bucalo – F. Pacini *Informazione e formazione del consenso politico,* in M.E. Bucalo – M. Caporale – A. Sterpa (a cura di), *Diritto pubblico di Internet,* Napoli, 2024, 253-282, nonché a M.E. Bucalo, *I volti della libertà di manifestazione nell'era digitale, fra intermediari online, moderazione dei contenuti e regolazione,* Torino, 2023.

[52] Percentuale che scende al 77% nel caso di *deepfake* generici. I dati sono del Garante per la Protezione dei dati Personali, *Vademecum* 2020. Quanto alla dottrina si veda H. Kshetri, *The Economics of Deepfakes*, in *Computing's Economics*, 2023, 89 ss.; G. Macgregor, *Gun to your head: how deepfakes and other non-consensual synthetic media hold individual autonomy hostage*, in *UMKC Law Review*, 2, 2021, 431 ss.

[53] Così V. Azzali – N. Ellecosta, *La questione deepfake in Italia, una panoramica,* in questa *Rivista*, 3, 2023, 82, che individua tale fattispecie nella «artificiale "deprivazione" di un individuo del proprio volto, seguita dalla sovrapposizione dello stesso a quello di un'altra persona.».
Oltre allo stato di angoscia in cui permango le vittime di *deepfake,* determinato dalla paura che il video o le immagini falsi possano continuare a essere presenti sul *web* e ritenuti autentici, è bene rilevare anche che in un *report* della organizzazione *Home Security Heroes* pubblicato negli Stati Uniti nel 2024, è emerso che il 74% degli uomini che avevano consumato materiale pornografico *deepfake* non manifestasse sensi di colpa riguardo al proprio consumo. Tale dato è facilmente interpretabile nel senso di una pericolosa accettazione e normalizzazione per una parte significativa del pubblico di tali contenuti, come prodotti per l'intrattenimento per adulti.

4. Il moltiplicarsi dei casi di *deepfake* in Europa e negli Stati Uniti e i diversi modelli normativi predisposti a tutela delle vittime

La disponibilità crescente delle applicazioni, scaricabili gratuitamente su ogni dispositivo, attraverso le quali è possibile creare *deepnude* e la facilità del loro utilizzo, sono divenute evidenti in recentissimi casi di cronaca avvenuti in Spagna, in Italia e negli Stati Uniti.

Nel mese di settembre 2023 nella cittadina spagnola di Alendralejo una ventina di ragazzine minorenni hanno trovato in circolazione sul *web* video modificati con programmi di Intelligenza Artificiale che le ritraevano nude e coinvolte in atti sessualmente espliciti. I filmati, che mostrano il viso delle minori su corpi sconosciuti, sono stati condivisi in *chat Whatsapp* e su *Telegram*. La vicenda, resa nota dopo la denuncia delle madri delle vittime, che, oltre a rivolgersi alle autorità spagnole, si sono riversate sui *social* per condannare l'accaduto, ha portato alla luce le responsabilità della creazione e divulgazione dei video erano dei compagni di scuola delle vittime**,** anche loro minorenni.

In Italia un caso analogo si è verificato a marzo 2023, quando due ragazzi di una scuola superiore di Latina hanno "spogliato per scherzo" cinque compagne di classe e una docente per mezzo della *app BikiniOff*[54].

L'episodio appena citato è peraltro analogo a quello successo sempre a Latina, in un'altra scuola superiore, esattamente un anno dopo, quando tre ragazzi minorenni, oggi indagati, hanno analogamente usato delle foto di due compagne per "spogliarle" usando la medesima l'*app*. Anche in questo caso i fotomontaggi delle due studentesse nude sono stati poi condivisi attraverso *chat* e *social network* tanto che, in poche ore, sono diventate virali all'interno dell'istituto[55].

Come è chiaro dagli esempi sopra riportati, tali usi della l'Intelligenza Artificiale sono in grado di impattare con la libertà di espressione (specialmente laddove tali forme espressive vengano poi diffuse su piattaforme digitali e dunque abbiano una diffusione globale) e, laddove si tratti dei *deepfake pornografici,* ripropongono e amplificano

[54] *BikiniOff* è una applicazione particolarmente apprezzata nel mondo dei *deepfaker,* poiché va oltre la mera sostituzione del viso, ricreando in modo sorprendentemente realistico la posa desiderata, mantenendo le proporzioni e il colore della pelle della vittima. Il *deepnude* della docente risultò peraltro così convincente da comparire su due siti pornografici. Sul caso si vedano D. Barbera, *Tutti i rischi di usare Bikinioff, il chatbot che spoglia le donne*, in *wired.it*, 19 aprile 2023 e S. Matteis, *Cinque 13enni e una prof di Latina nude sul web: indagati i compagni, le foto false create con l'app BikiniOff*, in *fanpage.it*, 14 settembre 2023.

[55] In seguito ai sopracitati eventi verificatisi a Latina, la Procura dei Minori di Roma ha avviato due diverse inchieste e il Garante per la protezione dei dati personali ha avviato un'istruttoria nei confronti di *Telegram* e ha mantenuto alta la attenzione sul tema stilando anche un *vademecum* intitolato *Deepfake. Il falso che ti "ruba" la faccia (e la privacy)*, emettendo provvedimenti, documenti ufficiali e comunicati., affrontando il tema del diritto alla identità personale anche in ottica divulgativa, proprio per il costante emergere di nuove tecnologie.
Casi del genere si stanno peraltro velocemente moltiplicando in tutto il mondo. A maggio 2023, per esempio, una bufala girava sul *web*: si trattava della foto di una avvenente giovane donna con *decolté* importante esibito in una occasione pubblica e che veniva spacciata per il ministro giapponese della salute**.** In realtà il ministro giapponese della salute era un uomo di mezza età e l'immagine della donna non era reale ma creata dalla IA della piattaforma *ChatGPT*. Si veda K. Hao, *Deepfake porn is ruining women's lives. Now the law may finally ban it*, in *technologyreview.com*, 12 febbraio 2021; H. Laffier – A. Rehaman, *Deepfakes and Harm to Women*, in *Digital Life and Learning*, 1, 2023.

esponenzialmente il problema della discriminazione di genere, integrando peraltro ipotesi di reato.

Analogamente negli Stati Uniti, sta sollevando questioni legali e morali indubbiamente urgenti il caso di due adolescenti, che nello scorso anno sono stati arrestati in Florida in base ad una legge del 2022, che ha istituito il reato di diffusione di immagini sessualmente esplicite senza il consenso della vittima. I due, infatti, avevano creato e diffuso immagini *deepfake* di nudi, utilizzando l'IA per generare rappresentazioni esplicite dei loro compagni di classe minorenni.

Nonostante ciò, il fenomeno dei nudi e delle immagini esplicite generate dall'IA da parte di minori sta diventando un problema sempre più comune nei distretti scolastici degli Stati Uniti, tanto che anche altri Stati si sono dotati di leggi analoghe a quelle della Florida.

In Virginia, per esempio, una legge del 2014 puniva la diffusione di foto o video con l'intento di costringere, molestare o intimidire un'altra persona. Nel 2019, tale legge è stata emendata estendendo la fattispecie e includendovi video o immagini statiche false e prevendendo una pena fino a un anno e una multa fino a 2500 dollari.

Analogamente in California nel 2019 sono state approvate due leggi in tema di *deepfake*: una prima che punisce chi pubblica video o immagini manipolate dei politici con l'intento di screditarli nei 60 giorni che precedono un'elezione che li vede coinvolti e una seconda che, invece, permette a chi si ritrova suo malgrado protagonista di un video *hard*, pur non avendone mai girato uno, di fare causa all'autore del *deepfake*.

Pur non di meno, negli Stati Uniti non esiste una legge di livello federale che affronti specificatamente il tema dei nudi *deepfake* non consensuali, lasciando dunque ai singoli Stati il compito di gestire, autonomamente, l'impatto dell'IA generativa su questioni delicate come il materiale di abuso sessuale infantile, il *revenge porn* e la formazione del consenso a fini politici.

A tal fine, il 30 ottobre 2023, il presidente Biden aveva emesso un ordine esecutivo[56], incaricando il Dipartimento del Commercio di sviluppare linee guida sul *watermarking* dei contenuti generati dall'IA, al fine di segnalare quando un contenuto multimediale è stato creato artificialmente e come è stato successivamente modificato[57].

A tal fine, l'ordine delegava ai Dipartimenti e alle Agenzie il ruolo essenziale di definire le linee guida, nonché eventuali standard di sicurezza generali, puntando sulla formazione, sullo sviluppo e sulla collaborazione volontaria delle imprese per raggiungere la trasparenza e l'affidabilità dei sistemi.

Quanto al sistema di marchiatura dei contenuti, esso oggi assolve essenzialmente a due funzioni. In primo luogo, esso può essere utilizzato per segnalare al fruitore di un'immagine, di un video o di un documento quale sia il suo vero autore, fungendo così da equivalente grafico del *copyright*. In questo caso, è usato come marchio per definire la proprietà di un prodotto audiovisivo.

---

[56] Executive Order 14110 of October 30, 2023 *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*.

[57] Per *watermarking* si intende la "marchiatura" dei contenuti volta a identificarne gli autori e la autenticità. La pratica è tutt'altro che recente: suoi precursori *ante litteram* sono per esempio la filigrana nella carta, nelle marche da bollo e nelle banconote dal XIII secolo in avanti.

Accanto a tale funzione tradizionale, ne esiste un'altra che sta acquisendo sempre più rilevanza, visti i recenti sviluppi dell'Intelligenza Artificiale e dei suoi possibili impieghi. L'applicazione di questa firma digitale, infatti, può costituire un valido strumento, per aiutare l'utente a distinguere un'immagine reale da una artificiale, potendo anche essere invisibile e inserita senza che l'immagine subisca alcun tipo di cambiamento percepibile, mantenendo inalterata la loro qualità e la fruibilità venga alterata[58].

La spinta americana sulla tecnologia *watermarking* evidenziava dunque un approccio molto diverso al problema da parte degli Stati Uniti, rispetto a quanto non stesse accadendo nell'Unione europea con l'approvazione del *AI Act*. Esso, infatti, appariva orientato a favorire le imprese e lo sviluppo dei sistemi di IA, che hanno da sempre un impatto politico decisivo, godendo di un forte sostegno da parte del Governo, con il quale sono interconnesse.

Tale approccio, da un lato, incentivava la frammentazione legislativa, spingendo i singoli Stati ad approvare per sé leggi spesso molto diverse, dall'altro la scelta di non dotarsi di una stringente regolazione del fenomeno era volta ad evitare di porre limiti allo sviluppo della tecnologia IA e alla competitività delle imprese americane impegnate nel settore. Analogamente succede per la manifestazione del pensiero sulle piattaforme digitale che negli Stati Uniti non è regolata in modo uniforme a livello federale[59], manifestandosi anche in quella sede un approccio maggiormente *business friendly* in favore delle aziende di quanto non accada, come vedremo, in Europa.

Le linee guida fissate dal citato ordine esecutivo sono state oggi abrogate dal presidente Trump il 23 gennaio 2025 con un nuovo ordine esecutivo[60], che evidentemente manifesta la volontà della nuova amministrazione di sviluppare un approccio del tutto libero e non regolamentato della evoluzione di tale tecnologia.

Ciò, da un lato, certamente accelera l'innovazione e attrae investimenti nel settore da parte di quelle aziende che si occupano di sviluppare l'IA; dall'altro, però, numerosi sono i rischi che tale politica determina quanto ai diritti degli utenti, soprattutto in relazione alla possibile proliferazione di contenuti falsi e disinformativi e non facilmente individuabili come tali, cui si aggiungono quelli relativi alle possibili discriminazioni algoritmiche e alle violazioni della privacy, che potrebbero ingenerare la sfiducia del consumatore verso questa tecnologia.

Per questo la sfida, cui la nuova deregolamentazione statunitense dovrà far fronte, sarà quella di trovare un equilibrio fra il sostegno allo sviluppo tecnologico, la minimizzazione dei rischi e la tutela dei diritti degli utenti.

Deve comunque segnalarsi che, dopo il caso occorso alla popstar Taylor Swift e in considerazione del fatto che cominciano a moltiplicarsi le azioni giudiziarie delle vittime del fenomeno soprattutto negli Stati che non si sono ancora dotati di una pro-

[58] Nonostante la sua utilità, un *report* intitolato *Detecting AI fingerprints: A guide to watermarking and beyond* del centro di ricerca americano *Brooking Institute* del gennaio 2024 sull'uso del *watermarking* in relazione all'IA sottolinea però come tale strumento di firma non sia privo di margini di errore, perché una volta inserito non è difficile da rimuovere per chi possieda le competenze per farlo.

[59] Anche qui si permetta di rinviare a M.E. Bucalo, *I volti della libertà di manifestazione del pensiero,* cit.

[60] Executive Order 14179 of January 23, 2025 *Removing Barriers to American Leadership in Artificial Intelligence*.

pria legislazione[61], il 30 gennaio 2024 al Congresso statunitense è stata presentata una proposta di legge detta *Defiance Act* (*Disrupt Explicit Forged Images And Non-Consensual Edits)*[62], che mira a fornire una disciplina unitaria del fenomeno, consentendo alle vittime di *deepfake* di richiedere un risarcimento a coloro che producono o possiedono intenzionalmente tali immagini con l'intento di propagarle.

Il modello di rimedi predisposti in Europa appare *ictu oculi* molto diverso da quello statunitense[63].

Volendo analizzare il modello italiano, esso, a differenza di quello statunitense, predispone già nel codice penale fattispecie generiche applicabili ai casi di diffusione di *deepfake* (anche pornografici): si tratta della sostituzione di persona di cui all'art. 494 c.p. e della frode informatica *ex* art. 640 *ter*, c. 3, c.p.

Quanto alla prima disposizione, che sanziona con la reclusione fino a un anno «chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici», la giurisprudenza della Corte di cassazione si è premurata di ricomprendervi anche condotte poste in essere mediante le nuove tecnologie, ed in particolare la creazione di un *account* sui *social network* utilizzando abusivamente l'immagine di una persona inconsapevole, associata ad un *nickname* di fantasia ed a caratteristiche personali negative[64].

La frode informatica sanziona, invece, con la reclusione da sei mesi a tre anni la condotta di colui il quale procura a sé o ad altri un ingiusto profitto con altrui danno «alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico». Ad essa l'art. 9, c. 1, lett. a), del d.l. 14 agosto 2013, n. 93, convertito dalla l. 15 ottobre 2013, n. 119, ha poi aggiunto un c. 3, che stabilisce una pena maggiore, per chiunque ponga in essere la condotta con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti. Disciplinando dunque il furto d'identità digitale, la norma citata è quella che nell'ordinamento italiano più si avvicina alla qualificazione del *deepfake* come illecito.

A tali fattispecie generiche, si somma il reato di "Diffusione illecita di immagini o video sessualmente espliciti", comunemente detto *revenge porn*[65], di cui all'art. 612 ter c.p., introdotto

[61] Nel New Jersey, che non ha una propria legislazione in tema, per esempio, i casi di *deepfake* porno sono proliferati nei licei, tanto che un adolescente ha citato in giudizio un compagno di classe per aver condiviso falsi nudi realizzati con l'IA. Su questi casi si veda l'articolo pubblicato su CBS news del 2 novembre 2023.

[62] S. 3696 – 118th Congress (2023-2024). Il testo risulta fermo presso il Senato dalla fine di luglio 2024.

[63] Le ragioni profonde che determinano tali diversità negli approcci fra le due sponde dell'Atlantico, sia a livello giurisprudenziale sia a livello regolatorio, sono note e possono essere brevemente riassunte nella tutela costituzionale, che potremmo definire "rafforzata", che il primo emendamento della Costituzione degli Stati Uniti assicura alla libertà di manifestazione del pensiero, a fronte del quale il vecchio continente oppone una visione che bilancia caso per caso la medesima libertà con gli altri diritti che con essa eventualmente entrassero in conflitto.

[64] Cass. pen., sez. V, 16 giugno 2014, n. 25774.

[65] Sulla correttezza della intitolazione informale del suddetto reato quale "*revenge porn*" è in corso il dibattito fra chi, soprattutto in ambienti giornalistici, lo ritiene un valido abbreviativo per individuare

dalla l. n. 69 del 2019, proprio per cercare di fronteggiare il fenomeno della diffusione di immagini e video sessuali senza il consenso della persona in questione, a seguito di riproduzione o sottrazione fraudolenta, e che prevede a tal fine la reclusione da uno a sei anni e la multa da 5.000 a 15.00 euro.

La previsione specifica di tale reato è presente solo in pochissimi ordinamenti al mondo ed in particolare, oltre che in Italia anche in Australia, Canada, Filippine, Giappone, Israele, Malta, Regno Unito e in alcuni Stati degli Stati Uniti.

Il tratto distintivo della norma risiede nella molteplicità dei destinatari della stessa. Infatti, l'articolo non mira a sanzionare soltanto coloro i quali abbiano diffuso i contenuti dopo averli personalmente realizzati o sottratti, ma anche tutti quei soggetti che, pur non avendo materialmente contribuito alla produzione o al furto degli stessi, abbiano contribuito a farli circolare dopo averli semplicemente ricevuti.

Ovviamente, condizione essenziale per l'applicazione è l'assenza del consenso della persona rappresentata, da intendersi cioè come manifestazione di volontà positiva ed esplicita. Infine, ai commi 3 e 4, l'articolo 612 ter c.p. prevede degli inasprimenti delle sanzioni nel caso di integrazione della fattispecie in situazioni particolarmente gravi, consistenti cioè in una relazione affettiva tra il reo e la vittima, o una condizione di inferiorità fisica o psichica della stessa.

La particolare attenzione rivolta in Italia a fattispecie come quelle sopra trattate è evidenziata anche dalla adozione di un altro strumento di "natura stragiudiziale", che imprime una notevole accelerazione alla loro risoluzione, evitando o comunque prevenendo la lunghezza dei tempi della giustizia. Si tratta dell'accordo concluso nel 2021 fra *Facebook* e Garante per la Privacy, in tema di pornografia *on line* non consensuale, che consente alle possibili vittime di iniziare un procedimento di segnalazione urgente, con un accesso privilegiato dal sito istituzionale del Garante stesso[66].

A tal fine, l'utente deve segnalare i *link* e i *post* da rimuovere e allegare le foto. Il sistema di collegamento fra Garante e *Facebook* consente quindi a quest'ultimo di individuare le foto allegate con velocità, cifrarle, rendendole così irriconoscibili e distruggerle, nonché attraverso una tecnologia di comparazione bloccarne le possibili condivisioni e nuove pubblicazioni anche su altre piattaforme

5. I *deepfake* in quanto "successori" delle *fake news*

La oggettiva gravità dei fatti trattati nel precedente paragrafo, rimarcata dalla potenza del mezzo informatico capace di diffonderne la lesività a livello globale, pone in luce anche il ruolo svolto dalle piattaforme *online*, veri signori delle porte di accesso alla rete (*Gatekeepers*), i quali forniscono gli strumenti e i servizi, che agevolano la diffusione di *deepfake*.

A fronte di tutto ciò, bisogna però rilevare la crescente pressione dell'opinione pubbli-

immediatamente la fattispecie e chi invece sostiene che essa, dal punto di vista giuridico e sociale, sia fuorviante e possa prestarsi ad interpretazioni pericolose e a derive che potrebbero in qualche modo tentare di giustificare questi atti. La vendetta, per quanto possa essere in astratto discutibile, presuppone infatti il fatto che esista alla base un torto o uno sgarbo per cui vendicarsi, cosa che in effetti non è. Si veda in tema *ex multis* G.M. Caletti, *"Revenge porn" e tutela penale*, in *Diritto Penale Contemporaneo Rivista Trimestrale,* 3, 2018, 63 ss.; F. Florio, *Non chiamatelo "revenge porn",* Milano, 2022; E. Strighi, *Revenge porn: lettura di genere di una fattispecie (incompresa),* in *Sociologia del diritto,* 1, 2021, 33 ss.

[66] Si veda la apposita pagina dedicata sul sito del Garante della protezione dei dati personali.

ca, volta a costringere le società di informazione a limitare la diffusione di tali contenuti e ad assumersene le relative responsabilità. A tale pressione, in prima battuta, pare aver dato risposta la Corte di Giustizia dell'Unione europea, che, in tema di *fake news*, ha oramai assunto come principio generale quello della responsabilità del *provider*.

A ben vedere tale principio, oramai consolidato nella giurisprudenza unionale, risulta applicabile anche ai *deepfake*, che a buon diritto possono essere considerati i "successori" tecnologicamente evoluti delle *fake news*.

In anni recenti, infatti, il fenomeno della disinformazione si è sviluppato in modo significativo non solo a causa dell'espansione di *Internet* e delle strategie di comunicazione digitale, ma anche grazie allo sviluppo e alla diffusione dei sistemi di IA[67].

Fra *fake news* e *deepfake* esistono infatti molti punti di contatto e molte analogie, a cominciare per esempio dalle difficoltà definitorie, che riguardano le prime e che sono analoghe per i secondi[68].

Vero è che le prime trovano il loro archetipo nelle bufale di età digitale, che esistono da sempre[69], ma è altrettanto vero che la cifra distintiva fra queste ultime e le attuali *fake news* è che nell'ecosistema digitale la diffusione di questi fenomeni assume una velocità mai avuta in età analogica. Per questo non si può che concordare con chi sostiene che «il maggior discrimine fra le *fake news* del passato e quelle attuali sta proprio nella "cinetica" con la quale si propagano al punto da costituire un elemento ontologico dirimente»[70].

Analogamente ciò può dirsi mettendo a raffronto *fake news* e *deepfake,* poiché analoghe sono le ragioni che determinano tale velocità di diffusione e che possono brevemente riassumersi nell'assetto oligopolistico degli *Internet Service Providers*, nel decentramento

[67] Sul punto O. Pollicino – P. Dunn, *Disinformazione e intelligenza artificiale nell'anno delle global election: rischi (ed opportunità),* in *federalismi.it,* 12, 2024, ix, i quali si soffermano sulla capacità dei sistemi di IA di produrre disinformazione, facendo riferimento, per il primo profilo, all'emersione di innumerevoli sistemi, legati in particolare alla cosiddetta "IA generativa", ai modelli fondativi e ai *large language models* (LLM), capaci di creare immagini, video e testi sintetici altamente realistici.

[68] Laddove si volesse tentare di definire il fenomeno delle *fake news*, secondo H. Allcott – M. Gentzkkow, *Social Media and Fake news in the 2016 elections*, in *Journal of Economic Perspectives,* 2, 2017, 211 ss., potrebbero intendersi quelle notizie che sono intenzionalmente e verificabilmente false e potrebbero trarre in inganno chi vi si imbatte. Verrebbero così escluse tutte le informazioni che, pur vicine al concetto di *fake*, non lo sono, collocandosi nel territorio del pensiero manifestato liberamente, ma si inserirebbero a buon diritto tutte le notizie false, costruite ad arte da gruppi di potere con l'obiettivo di modificare l'agenda pubblica, manipolando l'informazione e la formazione dell'opinione pubblica anche tramite tecnologie sofisticate, nonché tutte le notizie false che ledono interessi individuali o collettivi.

[69] Si ricordi per esempio che H. Von Kleist scrisse nel 1809 *Manuale dell'informazione francese*, una satira in risposta alla propaganda di guerra di Napoleone, nel quale descriveva come i giornali francesi montavano e diffondevano bufale, finalizzate solo ad esaltare l'imperatore. Leggendo R. Dale, *'Napoleon is Dead': Lord Cochrane and the Great Stock Exchange Scandal*, Londra, 2007 si scopre che la bufala della morte di Napoleone fu in grado di dirottare grandi capitali in borsa e fare decollare i titoli di Stato. Anche negli Stati Uniti le bufale esistevano già nel XIX sec., una fake news divenuta famosa fu quella che è stata chiamata la "Great Moon Hoax". Nel 1835 il New York Times pubblicava una serie di articoli che parlavano della scoperta della vita sulla Luna, falsamente attribuite a sir John Herschel, il più noto astronomo del tempo. L'idea dell'anonimo autore degli articoli, poi rivelatosi Richard Adams Locke, era presumibilmente solo quella di fare satira, che tuttavia fu creduta vera, sebbene le notizie suscitarono notevole scalpore e furono tradotti in diverse lingue nel mondo.

[70] Per questo non si può che concordare con A. Sciortino, *Fake news e post-verità nella società dell'algoritmo*, in *dirittifondamentali.it,* 2, 2021, 426.

della produzione della informazione, che non è più soggetta ai controlli legalmente imposti agli editori[71] e nella progressiva perdita di fiducia in tv e carta stampata come strumenti di informazione, utili per il confronto fra opinioni diverse, ma oramai tacciate di parzialità e commistione con gli apparati pubblici o con i grandi poteri economici[72].
Epperò i *deepfake* possono considerarsi una evoluzione, in senso peggiorativo, delle *fake news,* considerato che essi associano alla "cinetica" della loro propagazione attraverso *Internet,* anche un "aggravamento" della falsità in quanto l'immagine (o il video) ha un impatto certamente maggiore sull'utente della Rete, di quanto non lo abbiano le opinioni o gli scritti[73]. A tutto ciò, che evidentemente accelera ulteriormente la diffusione, si somma la preoccupante considerazione che l'uso della IA rende ancor più difficilmente distinguibile ciò che è veritiero visivamente da ciò che non lo è.
Ancora, deve segnalarsi come per le *fake news*, la peculiare organizzazione dei contenuti in *Internet*, che si fonda su sistemi di raccomandazione (*recommender* o *recommendation systems*) i quali, partendo dai dati e dalle informazioni raccolte sulle preferenze del singolo utente, sono in grado di predirne l'indice di gradimento con riferimento a nuovi contenuti ed elementi[74].
Tale sistema di diffusione delle informazioni *online* presenta certamente il pregio di poter essere usato proattivamente al fine di garantire una diffusione dei contenuti quanto più plurale possibile, ma anche un effetto collaterale. Poiché infatti a muovere l'*engagement* degli utenti da parte dei gestori delle piattaforme è sostanzialmente il loro interesse economico e poiché i contenuti altamente divisivi e polarizzanti, come si diceva, tendono ad attrarre maggiormente l'attenzione del pubblico, esiste il concreto rischio che «l'algoritmo, pur di suscitare l'interesse degli utenti, sia disincentivato a ridurre la diffusione di disinformazione»[75].
I rischi sono poi ulteriormente accentuati dal meccanismo di filtraggio che viene operato dalle piattaforme e dai *social network* nella pubblicazione e nella diffusione dei contenuti. La semplice navigazione degli utenti, infatti, determina da parte dei gestori la raccolta dei loro dati, profilati poi per mezzo di operazioni algoritmiche. In tal modo essi sono in grado, per così dire, di "predire" in futuro i comportamenti individuali e collettivi degli utenti e conseguentemente di influenzarne le decisioni.

---

[71] G.E. Vigevani, *L'informazione e i suoi limiti: il diritto di cronaca*, in G.E. Vigevani – O. Pollicino – C. Melzi D'Eril – M. Cuniberti – M. Bassini, *Diritto dell'informazione e dei media*, Torino, 2019, 25 ss.

[72] Si veda in tema G. Pitruzzella, *Libertà di manifestazione del pensiero nell'era di Internet*, in G. Pitruzzella – O. Pollicino – S. Quintarelli, *Parole e potere. Libertà di espressione*, hate speech *e* fake news, Milano, 2017, 70 ss.

[73] O. Pollicino – P. Dunn, *Disinformazione e intelligenza artificiale,* cit., ix-x. e xii, affermano che «quanto alla "disseminazione" di *deepfake online* va rilevato che, da un lato l'IA viene utilizzata dai produttori o da soggetti comunque interessati alla diffusione di materiali falsi in rete al fine precipuo di aumentarne l'impatto» e ritengono particolarmente diffusa «la pratica di ricorrere a *social bot*, ovverosia ad *account* falsi gestiti in modo automatico o semiautomatico (in quest'ultimo caso si parla di "*cyborg*", cioè di profili gestiti in parte da persone vere e in parte dall'IA) con il preciso obiettivo di contribuire alla diffusione di materiali "inquinanti"».

[74] Secondo O. Pollicino – P. Dunn, *Disinformazione e intelligenza artificiale,* cit.,xiii, tali sistemi svolgono un ruolo centrale nella diffusione delle informazioni e, pertanto, nella formazione della stessa coscienza pubblica, avendo la capacità di influenzare e strutturare le stesse preferenze degli utenti e di guidarne le scelte sia a livello individuale sia a livello sociale e collettivo.

[75] Ivi, xiii.

Da un lato le attività della vita degli utenti sono registrate ogni volta che si connettono a *Internet*, perché i dati che costoro lasciano nella Rete restituiscono un loro "profilo" utile poi alle piattaforme per indirizzarli nelle ricerche successive. Dall'altro però, il procedimento seguito per aggregare gli "indizi" relativi alla loro personalità (i dati appunto), che "prediranno" i comportamenti futuri, è del tutto oscuro (*black box society*)[76].
La profilazione dei contenuti determina come immediata conseguenza anche la personalizzazione delle informazioni, operata per ciascun utente dagli stessi motori di ricerca e *social network*, i quali rendono disponibili le informazioni ricercate secondo un *ranking,* il cui ordine è stabilito per mezzo delle stesse operazioni algoritmiche che hanno contribuito alla sua profilazione.
Così, se le notizie, i contenuti o i risultati delle ricerche sono profilati in modo da "predire" la personalità dell'utente, allora quest'ultimo visualizzerà sempre e solo quelle informazioni conformi al suo pensiero e si convincerà che nella realtà esistono soltanto persone, che esprimono le sue stesse idee. La possibilità di accedere a fonti di informazione o pareri che discordino da queste convinzioni sarà evidentemente molto limitata, come di conseguenza lo sarà anche la formazione di una opinione genuinamente consapevole.
Si tratta di un vero e proprio processo di «inscatolamento del nostro mondo informativo»[77] e della conseguente costruzione di mondi che sono solo a immagine e somiglianza di colui che naviga in Rete.
Volendo usare una nota metafora, ciascuno sembra chiuso in una *filter bubble*[78] (o anche *echo chamber*), che però «amplifica le divisioni e le polarizzazioni, tradendo una delle missioni più profonde della libertà di espressione e del confronto: la tolleranza reciproca fra opinioni differenti»[79].

6. I rimedi predisposti dalla giurisprudenza dell'Unione europea

Analizzando adesso i rimedi predisposti a fronte della diffusione *online* dei *deepfake* e rivolgendo l'attenzione in prima battuta alla giurisprudenza dell'Unione europea, è noto che il modello decisorio della Corte di Giustizia risente, oltre che della assenza di una disciplina specifica (sanata solo nel 2023 con l'approvazione del *Digital Service Package*), anche della genesi del suo ordinamento, improntata ad una visione prettamen-

[76] Sul punto si veda F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard, 2015, 9 ss. Sulla "doppia natura" conoscitiva e predittiva dell'algoritmo, nonché sulla necessità di regole che ne assicurino la trasparenza e il rispetto dei diritti degli utenti della Rete, prima fra tutte la privacy si veda anche L. Torchia, *Stato digitale*, cit., 24-25. Analogamente, A. Koltay, *New Media and Freedom of Expression: Rethinking the Constitutional Foundation of Public Sphere*, Oxford, 2021, 86.

[77] M. Calise – F. Musella, *Il Principe digitale*, Roma-Bari, 2019, 11.

[78] E. Parisier, *Filter Bubble: How the New Personalized Web Is Changing What We Read and how We Think*, New York, 2011.

[79] C. Bologna, *Libera di espressione e "riservatezza" nella Rete? Alcune osservazioni sul mercato delle idee nell'agorà digitale*, in *Rivista del Gruppo di Pisa*, fascicolo speciale, 3, 2021, 71.

te mercantilistica dei diritti fondamentali e della loro tutela[80]. Ciò ha determinato una giurisprudenza, che si occupa del tema in modo, per così dire, indiretto, improntata al bilanciamento fra il diritto di espressione e gli altri diritti di estrazione economica, spesso ritenuti prevalenti o comunque dotati di una tutela rafforzata.

Fra questi il primo che va certamente menzionato è il diritto alla *privacy*[81], la cui tutela nell'ambito della società dell'informazione aveva stimolato il ruolo di supplenza della Corte di Giustizia, in considerazione della perdurante inerzia del legislatore europeo nell'opera di necessario aggiornamento della disciplina previgente.

L'archetipo di questo filone giurisprudenziale è la sentenza *Lindqvist*[82], con la quale per la prima volta la Corte di Giustizia definì l'ambito di applicazione della Direttiva 95/46 in tema di privacy (previgente rispetto al GDPR) nel quadro del nuovo scenario tecnologico, nonché indagare il rapporto fra protezione dei dati personali e libertà di espressione[83].

Volendo assicurare alla tutela dei dati personali una protezione a tutto tondo, la Corte affermava che il bilanciamento fra tutela della *privacy* e le altre libertà, andava effettuato caso per caso e che era compito delle autorità nazionali e dei giudici non solo interpretare il diritto nazionale in conformità con la direttiva 65/46, ma anche «provvedere a non fondarsi su un'interpretazione di quest'ultima che entri in conflitto con i diritti fondamentali tutelati nell'ordinamento giuridico comunitario»[84].

L'altra pronuncia "archetipo" [85] da menzionare necessariamente in questa sede è quella che determinò l'annullamento della direttiva 2006/24/CE (c.d. "*Data Retention*") relativa alla conservazione dei dati di traffico per violazione degli artt. 7 e 8 della Carta europea dei diritti fondamentali[86].

---

[80] M. Bassini, *Internet e libertà di espressione. Prospettive costituzionali nazionali e sovranazionali*, Roma, 2019, 319

[81] Il quale oggi gode, oltre che di una consolidata giurisprudenza, anche di una forte accelerazione impressagli dal GDPR del 2016, che ha sostituito la oramai risalente disciplina della direttiva 95/46/CE.

[82] CGUE, C-101/01, *Lindqvist* (2003). Sul punto si vedano i commenti di A. Palmieri – R. Pardolesi, *Il codice in materia di dati personali e l'intangibilità della* privacy *comunitaria*, in *Foro italiano*, 2, 2004, 59 ss.; T.M. Ubertazzi*, Il caso Lindqvist: i limiti della privacy*, in *Danno e responsabilità*, 24, 2004, 382 ss.

[83] Il caso riguardava la pubblicazione fatta da una cittadina svedese sul suo sito internet dei dati di alcune persone che lavoravano con lei come volontari in una parrocchia, senza averne ricevuto il consenso. Dopo la condanna in primo grado, la Corte di Appello aveva deciso di sollevare avanti la Corte di Giustizia sette questioni pregiudiziali riguardanti l'ambito di applicazione della direttiva sulla *privacy*, una delle quali espressamente chiedeva se la disciplina della direttiva potesse ritenersi compatibile con i principi generali in materia di libertà di espressione.

[84] CGUE, C-101/01, *Lindqvist* (2003), § 87.

[85] La pronuncia è infatti il fondamento della successiva giurisprudenza unionale in tema di tutela dei dati personali e da ultimo è stata recentemente ripresa *ex multis* da CGUE, C-746/18, *H.K. c. Prokuratuur* (2021) e CGUE, C-140/20, *G.D. contro The Commissioner of the Garda Síochána e a.* (2022).

[86] CGUE, C-293/12 e C-594/12, *Digital Rights Ireland Ltd e Kärntner Landesregierung* (2014). La sentenza è stata seguita dalla pronuncia sul caso analogo CGUE, C-203/15 e C-698/15, *Tele2Sverige* (2016). Moltissimi i commenti a questa sentenza. *Ex multis* R. Flor, *Dalla "data retention" al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive* "de jure condendo"?, in *Il diritto dell'informazione e dell'informatica*, 4-5, 2014, 775 ss.; L. Trucco, "Data retention*": la Corte di Giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giurisprudenza italiana*, 8-9, 2014, 1850 ss.; G. Tiberi*, La Corte di Giustizia sulla conservazione dei dati: la protezione dei diritti fondamentali nel "dopo-Lisbona"*, in *Quaderni costituzionali*, 3, 2014, 719 ss.; A. Arena, *La Corte di Giustizia*

La direttiva richiedeva agli Stati membri di conservare in modo generalizzato i dati di traffico connessi a qualsiasi mezzo comunicativo di tutti gli utenti, senza alcuna distinzione, limitazione o eccezione rispetto all'obiettivo di contrasto alla criminalità. Peraltro, l'archiviazione aveva ad oggetto dati di persone che, nemmeno indirettamente, si trovavano nella situazione di dare adito a procedimenti penali o di essere collegate, anche solo in modo remoto, a reati gravi.

La sentenza si rivelava di importanza fondamentale per la rilevanza che in essa assume il canone della proporzionalità delle misure limitative degli indicati diritti e che, nel caso di specie, non risultava rispettato, a causa della raccolta e conservazione generalizzata dei dati di tutti i soggetti, disposta dalla direttiva e che dunque risultava eccessivamente intrusiva rispetto ai diritti sanciti dalla Carta di Nizza.

È però la celebre sentenza *Google Spain*[87] a dimostrare in modo chiaro l'influenza della tecnologia digitale nel rapporto fra libertà di espressione e diritto alla protezione dei dati personali e ad individuare un primo possibile argine alla progressiva espansione del potere delle piattaforme nel cyberspazio, imponendo la loro responsabilità nella tutela del diritto alla privacy e degli altri diritti sanciti nella Carta di Nizza[88].

sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento, in *Quaderni costituzionali*, 3, 2014, 7872 ss.

[87] CGUE, C-131/12, *Google Spain* (2014). Moltissimi i commenti alla sentenza, se ne citano qui solo alcuni *ex plurimis* F. Pizzetti, *La decisione della Corte di Giustizia sul caso* Google Spain: *più problemi che soluzioni, in federalismi.it*, 12, 2014; T.E. Frosini*, Diritto all'oblio e Internet*, ivi; tutti i contributi nel volume G. Resta – V. Zeno-Zencovich (a cura di*), Il diritto all'oblio dopo la sentenza* Google Spain, Roma, 2015 fra i quali O. Pollicino, *Un* digital right to privacy *preso (troppo) sul serio*, ivi, 17 ss.; G. Finocchiaro*, Il diritto all'oblio nel quadro dei diritti della personalità,* ivi*,* 29 ss.; T.E. Frosini, *Google e il diritto all'oblio preso sul serio,* ivi*,* 1 ss.; O. Pollicino – M. Bassini*, Reconciling right to be forgotten and freedom of information in the digital age. Past and future of personal data protection in the European Union*, in *DPCE*, 2, 2014, 641 ss.; M. Bassini, Google *davanti alla Corte di Giustizia: il diritto all'oblio*, in *Quaderni costituzionali*, 3, 2014, 730 ss.; M.C. D'Arienzo, *I nuovi scenari della tutela della* privacy *nell'era della digitalizzazione alla luce delle recenti pronunce sul diritto all'oblio*, in *federalismi.it*, 2, 2015; L. De Grazia, *La libertà di stampa e il diritto all'oblio nei casi di diffusione di articoli attraverso Internet: argomenti comparativi*, in *Rivista AIC*, 4, 2013; S. Leucci, *Diritto all'oblio, verità, design tecnologico: una prospettiva di ricerca,* in questa *Rivista*, 1, 2017, 116 ss.; 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; R. Pastena, Internet *e* privacy: *una relazione complicata (A margine della sentenza della Corte di Giustizia del 13 maggio 2014)*, in *Osservatorio Aic*, 2, 2014; R.C. Post*, Data Privacy and Dignitary Privacy: Google Spain and the right to be forgotten, and the construction of public sphere*, in *Duke*, 2018, 981 ss.; E. Frantziou, *Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*, in *Human Rights Law Review*, 14, 2014, 76 ss. ; O. Spataro*, Il diritto all'oblio tra definizione sostanziale e rimedi di tutela. Riflessioni alla luce della giurisprudenza più recente della Corte di Cassazione e della Corte di Giustizia dell'Unione Europea in materia di deindicizzazione*, in *Diritto costituzionale*, 1, 2023, 133 ss.

[88] Per comprendere appieno la portata della pronuncia è necessario partire dalla fattispecie che la ha originata e che vedeva opposti un cittadino spagnolo e Google avanti l'Autorità spagnola per la protezione dei dati personali (*AEPD*). In particolare, il ricorrente sig. Costeja Gonzalez aveva chiesto che fosse ordinato al motore di ricerca di cancellare dalla pagina della ricerca alcuni link, che rimandavano ad una vicenda giudiziaria, in materia di pignoramenti immobiliari per debiti previdenziali, che lo aveva riguardato molti anni prima e che si era completamente conclusa. Analogamente lo stesso ricorrente chiedeva che fosse ordinato al giornale, che per ordine dell'autorità giudiziaria doveva dare massima pubblicità alla vicenda, di cancellare permanentemente le relative pagine o che ivi fossero occultati i suoi dati personali. Il Garante spagnolo aveva accolto il ricorso nella parte in cui chiedeva a *Google* di deindicizzare i link che riportavano al ricorrente, ma non quanto alla richiesta rivolta al quotidiano. Avverso questa decisione *Google* ricorreva avanti *l'Audiencia Nacional*, che sollevava alcune questioni pregiudiziali.

Le questioni sollevate dal remittente avevano ad oggetto, oltre che l'ambito territoriale di applicazione della allora vigente direttiva sulla *privacy*, l'identificazione della attività della piattaforma come trattamento dei dati personali, la portata dei diritti di cancellazione e opposizione al trattamento dei dati previsti dall'art. 12 lett. b) della direttiva stessa[89] e l'obbligo della stessa di rispettare i diritti umani determinandone la responsabilità.

Dopo aver affermato che le disposizioni in questione si applicano anche al soggetto o alla società che, pur non avendo sede nell'Unione, vi siano comunque stabiliti, determinando così la vigenza extraterritoriale e potenzialmente globale del diritto dell'Unione[90], la pronuncia si dedicava alla individuazione del ruolo svolto dalle piattaforme in ambiente digitale, ne identifica il potere e conseguentemente, vista l'estensione dello stesso, la piena responsabilità.

A tal fine la Corte identifica preliminarmente nei motori di ricerca i titolari del trattamento dei dati, perché li diffondono in modo globale, rendendoli accessibili a tutti gli utenti di *Internet*, li aggregano e li organizzano, in modo che l'utente che fa la ricerca possa averne una visione complessiva, e infine li conservano nei propri *server*[91].

Questa attività, che incide «in modo significativo […] sui diritti fondamentali di cui agli artt. 7 e 8 della Carta di Nizza», determina in capo al motore di ricerca l'obbligo di svolgerla in modo che le garanzie previste dalla direttiva 95/46 possano sviluppare pienamente i loro effetti[92].

Conseguenzialmente nel caso di mancato rispetto delle norme della direttiva stessa, ne consegue che il gestore del motore di ricerca ha l'obbligo di «sopprimere, dall'elenco di risultati [...] i link verso pagine web pubblicate da terzi e contenenti informazioni relative all'utente, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine» originarie, ancorché tali pubblicazioni siano lecite[93].

A tale responsabilità del *provider*, i giudici di Lussemburgo riconoscono allo stesso l'ulteriore obbligo di valutare in ordine alla sussistenza dei presupposti per l'esercizio del diritto e alla compatibilità con la libertà di informazione, che devono valutare caso per caso rilevando l'eventuale sussistenza di ragioni particolari, che determinerebbero il prevalere dell'interesse pubblico ad avere accesso all'informazione o meno[94].

La pronuncia però, come rilevato dalla dottrina maggioritaria, determinava il rischio di responsabilizzare eccessivamente il *provider,* che veniva indotto a cancellare il più

[89] Il quale disponeva che «Gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento: [...] a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati».

[90] Sul punto si veda G. Sartor – M. Viola De Azevedo Cunha, *Il caso Google e i rapporti regolatori USA/EU*, in G. Resta – V. Zeno-Zencovich (a cura di), *Il diritto all'oblio*, cit., 99 ss.

[91] CGUE, C-131/12, *Google Spain* (2014), §§ 36-38 e 83.

[92] Ivi, § 38.

[93] Ivi, §§ 70, 76 e 87-88.

[94] Ivi, § 97. Secondo M. Bassini, *Internet e libertà di espressione*, cit., 328, la Corte così sembra volere costruire intorno ai provider una responsabilità piena e a trecentosessanta gradi, rendendoli arbitri del conflitto fra i due diritti e affidando loro compiti difficilmente gestibili.

possibile le notizie, assegnandogli il compito di valutare ciò che può essere pubblicato e indicizzato perché di pubblico interesse e ciò che invece non lo è, facendo emergere il contrasto lampante con il principio costituzionale della riserva di giurisdizione nei casi di possibili restrizioni dei diritti fondamentali «che caratterizza il nucleo duro di qualsiasi ordinamento che si fondi sulla *rule of law*»[95].

D'altro canto, dalla sentenza citata anche la posizione degli utenti sembrava tutelata solo a metà, poiché ad essi era pienamente riconosciuto il diritto alla deindicizzazione, ma al contrario risultava gravemente leso il loro diritto all'informazione[96].

Alle ortodossie dimostrate dalla sentenza *Google Spain* sono stati posti dei correttivi con la sentenza *Google c. Commission Nationale de l'Informatique e des Libertes (CNIL – Autorità francese per la protezione dei dati personali)*[97], esito di un rinvio pregiudiziale promosso dal *Conseil d'Etat,* davanti al quale pendeva un ricorso avverso una decisione dell'Autorità del 2015, che aveva irrogato una sanzione nei confronti di *Google* a causa del diniego di operare una deindicizzazione su tutte le estensioni del nome a dominio del suo motore di ricerca e non già solo sulle declinazioni nazionali (.fr).

In questo caso la Corte di giustizia corregge parzialmente il tiro rispetto alla pronuncia *Google Spain*, affermando che l'obbligo di deindicizzazione gravasse sul *provider* e nella sua versione nazionale e nelle sue versioni relative ad altri Stati membri, ma certamente non potesse avere carattere globale, poiché, non esistendo un diritto alla deindicizzazione globale negli ordinamenti degli Stati, l'equilibrio fra diritto all'oblio e libertà di informazione degli utenti in Internet può «variare notevolmente nel mondo». Prova ne è il fatto che i singoli Stati membri possono prevedere discipline differenziate «in particolare per il trattamento a fini esclusivamente giornalistici o di espressione artistica o letteraria e per le esenzioni e le deroghe necessarie per conciliare tali diritti con la libertà di informazione»[98].

A questo ridimensionamento territoriale, non segue però alcun ridimensionamento degli obblighi e delle responsabilità del *provider*, al quale è comunque imposto di adottare le misure efficaci, affinché venga soddisfatto il bilanciamento fra i diritti fonda-

---

[95] O. Pollicino, *Un digital right to privacy preso (troppo) sul serio*, in G. Resta – V. Zeno-Zencovich (a cura di), *Il diritto all'oblio*, cit., 18.

[96] M. Bassini, *Internet e libertà di espressione*, cit., 339.

[97] CGUE, C-517/17, *Google v. CNIL* (2019). Fra i molti commenti F. Balducci Romano, *La Corte di giustizia "resetta" il diritto all'oblio*, in *federalismi.it*, 3, 2020, 3 ss.; A. Iannotti Della Valle, *Il diritto all'oblio "preso meno sul serio",* in *Rivista AIC*, 2, 2020, 495 ss.; G. Bellomo, *"Diritto all'oblio" e portata territoriale del "diritto alla deindicizzazione": la Corte ridisegna i confini applicativi*, in *DPCE online*, 4, 2019, 2987 ss.; G. Bevilacqua, *La dimensione territoriale dell'oblio in uno spazio globale e universale*, in *federalismi.it*, 23, 2019, 1 ss.; A. Correra, *La tutela dei dati personali e la portata territoriale dell'obbligo di deindicizzazione dei contenuti online*, in *Eurojus*, 3, 2020, 35 ss.; M. Orefice*, Diritto alla deindicizzazione: dimensione digitale e sovranità territoriale*, in *Rivista AIC*, 1, 2020, 653 ss.; F. Giovanella, *From the "right to delisting" to the "right to relisting"*, in questa *Rivista*, 2, 2022, 124 ss.; nonché e O. Spataro, *Il diritto all'oblio,* spec. 134 ss. Per la dottrina straniera, B. Martìn, *Google v. CNIL and the Right to Be Forgotten: A Judgment of Solomon*, in *Global Privacy Law Review*, 1, 2020, 61 ss.; M. Zalnieriute, Google LLC v. *Commission Nationale de l'Informatique et des Libertés (CNIL),* in *American Journal of International Law*, 2, 2020, 261 ss.; Y. Miadzvetskaya – G. Van Calster, *Google at the Kirchberg Dock. On Delisting Requests, and on the Territorial Reach of the EU's GDPR (C-136/17 GC and Others v CNIL, C□ 507/17 Google Inc v CNIL)*, in *European Data Protection Law Review*, 1, 2020, 143 ss.; O.J. Gstrein, *Right to be Forgotten: EU-ropean Data Imperialism, National Privilege, or Universal Human Right?,* in *Review of European Administrative Law (REALaw)*, 1, 2020, 125 ss.

[98] CGUE, C-517/17, *Google v. CNIL* (2019, § 67.

mentali e si impedisca agli utenti «di avere accesso ai link in questione a partire da una ricerca effettuata sulla base del nome»[99], conferendogli nuovamente una responsabilità *ultra vires*, che comporta il rischio della radicalizzazione della deindicizzazione e quello dell'attribuzione agli stessi di poteri gestori, che invece dovrebbero competere allo Stato e alla giurisdizione.

L'evoluzione e la razionalizzazione delle scelte giurisprudenziali europee in materia pare essersi compiuta solo con la sentenza *TU e RE c. Google*[100], che peraltro contiene assunti utili anche ai fini dell'individuazione delle responsabilità del *provider* in caso di *deepfake*.

Essa giunge all'esito di un rinvio pregiudiziale sollevato dalla Corte federale di Giustizia tedesca, avanti la quale avevano fatto ricorso due persone che avevano chiesto a *Google* di deindicizzare dall'elenco dei risultati di ricerca i *link* relativi ad alcuni articoli, apparsi su un sito che esponevano valutazioni critiche sul modello di investimento attuato da una società del loro gruppo, in quanto contenevano affermazioni inesatte e opinioni diffamatorie.

La questione posta, e che interessa particolarmente ai fini di questo studio, aveva riguardo al diritto alla deindicizzazione e chiedeva se la relativa richiesta potesse fondarsi sul fatto che le allegazioni contenute nel *link* fossero contestate nella loro veridicità dal ricorrente o se dovesse essere necessario un previo provvedimento giudiziario, che risolvesse la questione della attendibilità del contenuto visualizzato.

La Corte non pare discostarsi dalla sua precedente giurisprudenza e infatti ribadisce che l'attività del motore di ricerca deve essere qualificata "trattamento dei dati personali" ai sensi del GDPR e che dunque il gestore deve essere qualificato "responsabile del trattamento"[101].

Il dato in più, che costituisce la cifra distintiva della sentenza ora in analisi rispetto alle precedenti, è che la Corte sembra aggiungere nuovi criteri, a quelli già individuati, affinché il motore di ricerca proceda alla deindicizzazione. In particolare, essi sono individuabili nella falsità dell'informazione e nella sua palese inesattezza, le quali costituiscono «un elemento pertinente nell'ambito della valutazione delle condizioni di applicazione previste all'articolo 17, paragrafo 3, lettera a), del GDPR, al fine di valutare se il diritto all'informazione degli utenti di *Internet* e la libertà di espressione del fornitore di contenuti possano prevalere sui diritti del richiedente la deindicizzazione»[102].

L'idea che qui la Corte fa propria è quella che la falsità palese, l'inesattezza evidente non possono essere ricomprese nella libertà di informazione, perché «tale diritto, nella sua duplice valenza, attiva e passiva, se riferito ad un'informazione falsa, non può comunque essere posto sullo stesso piano dei diritti fondamentali al rispetto della vita

[99] Ivi, § 70.

[100] CGUE, C-460/20, *Tu. e Re. v. Google* (2022). Si veda G. Napoli, *Diritto alla deindicizzazione e notizie false: la Corte di giustizia precisa i confini tra oblio e libertà di espressione*, in questa *Rivista*, 1, 2023; F. Paolucci, I (Don't) remember my name: *il diritto all'oblio nella recente pronuncia C-460/2020 della Corte di Giustizia dell'Unione Europea,* in *Diritti Comparati*, 19 gennaio 2023.

[101] CGUE, C-460/20, *Tu. e Re. v. Google,* (2022), § 44.

[102] Ivi, § 64.

privata e alla tutela dei dati personali»[103]. Per far questo la prevalenza è assegnata alla dignità umana, in quanto valore fondamentale dell'Unione, rendendo di fatto inesistente il conflitto fra il diritto alla riservatezza e il diritto di espressione. In questo caso la richiesta di deindicizzazione potrà essere posta direttamente dall'interessato al motore di ricerca, poiché dal punto di vista probatorio, non è necessario che costui la accompagni con un previo provvedimento giurisdizionale (o amministrativo) che accerti l'inesattezza medesima o la falsità[104].

Si instaura così un rapporto diretto fra piattaforma e utente, cui segue anche una sorta di alleggerimento della posizione del *provider*, che evita anche i menzionati rischi di "deindicizzazione di massa", perché nel caso in cui il soggetto che ha presentato una siffatta richiesta, apportando elementi di prova pertinenti e sufficienti a dimostrare inesattezza o la falsità delle informazioni, il gestore del motore di ricerca sarà tenuto ad accogliere detta richiesta di deindicizzazione. Solo nel caso in cui tale inesattezza non risulti manifesta, avanti il rifiuto di deindicizzazione del gestore della piattaforma, l'utente dovrà adire l'autorità giudiziaria.

Anche la seconda questione posta nel medesimo rinvio interessa particolarmente la presente analisi, perché era relativa alla possibilità che la deindicizzazione potesse avere ad oggetto anche le foto di persone fisiche che, nell'ambito di una ricerca nominativa, fossero visualizzate come miniature (*"thumbnails"*) e dovesse tener conto in modo determinante del contesto della pubblicazione originaria, anche quando il motore di ricerca, visualizzando la miniatura, in effetti rimanda al sito originario, ma senza menzionarlo concretamente.

La Corte, dunque, imprime una marcia in più alla tutela della persona eventualmente lesa dalla pubblicazione delle immagini, perché esse rispetto alla comunicazione verbale hanno un impatto più forte sugli utenti di Internet, dunque, nella valutazione della richiesta di tale deindicizzazione deve essere attribuito loro un valore informativo superiore che prescinde dal contesto della loro pubblicazione nelle pagine *web* originarie[105].

---

[103] Così le conclusioni dell'Avvocato Generale Pitruzzella in C-460/20, § 30.

[104] Infatti, per evitare di far gravare sulla persona un eccessivo onere accertativo, la Corte afferma che essa sia tenuta unicamente a fornire elementi di prova, dei quali può ragionevolmente essere in possesso, atti a dimostrare l'inesattezza manifesta. CGUE, C-460/20, *Tu. e Re. v. Google* (2022), § 68.
Deve segnalarsi che il canone della falsità e dell'inesattezza come criteri identificativi della responsabilità delle piattaforme *online* e del loro obbligo di rimozione immediata dei contenuti pubblicati è posto fondamento anche della pronuncia del Tribunale di Milano, sez. I civ., 15 febbraio 2023, n. 1208, emessa in un procedimento per risarcimento del danno promosso dalla società *Snaitech* (nota concessionaria per la gestione dei giochi legali e autorizzati in Italia) contro *Facebook*.
In essa il *social network*, anche in considerazione dell'«ampia capacità diffusiva dei contenuti che ospitano le piattaforme c.d. social» (12-13), viene condannato al risarcimento del danno per non aver rimosso le pagine recanti post palesemente falsi, sulla base della costatazione per la quale il «diritto di critica, il quale costituisce notoriamente espressione della libertà di manifestazione del pensiero di matrice costituzionale (art. 21 Cost.)» non è configurabile nel caso in cui il contraddittore aggredisca «con accuse di perpetrazione di veri e propri delitti o comunque di condotte infamanti in rapporto alla dimensione personale, sociale o professionale del destinatario» (11).

[105] CGUE, C-460/20, *Tu e Re. v. Google* (2022), § 85.

7. I rimedi predisposti dal diritto positivo dell'Unione europea

7.1 Il Digital Market Package

Quanto invece ai rimedi diritto positivo avverso la diffusione di *deepfake* e *deep porn,* deve segnalarsi come l'Unione europea sia stata la prima nel panorama globale a dotarsi di una normazione in materia di mercati e servizi digitali resi dalle società di informazione, garantendo peraltro alle vittime di *deepfake* strumenti di tutela ulteriori rispetto alla possibilità di adire la autorità giudiziaria, adeguati alla velocità con la quale si diffondono *online* tali contenuti dannosi[106].

Ci si riferisce al *Digital Markets Package*, oggi integrato dal regolamento *Artificial Intelligence Act.*

Il primo è un pacchetto di due regolamenti*,* in vigore dal mese di maggio 2023 (*Digital Market Act*[107] e *Digital Service Act*[108]), che delinea un modello di intervento regolativo che mira a contemperare, da un lato, le esigenze dello sviluppo economico del settore digitale e la capacità di innovazione del tessuto imprenditoriale europeo, e, dall'altro, gli interessi economici e politici dell'Unione; esso si caratterizza anche per la precisa scelta normativa di prediligere norme di carattere prevalentemente procedurale o procedimentale, che procedono di pari passo con un più generale quadro assiologico, fondato sui valori dell'Unione europea[109].

La scelta dello strumento normativo, il regolamento e non la direttiva, latore di norme armonizzate e direttamente applicabili, manifesta la volontà del legislatore europeo, volta a riaccentrare la disciplina di materie così complesse nelle sue mani[110] e ad evitare la frammentazione normativa a livello dei singoli Stati membri[111], pervenendo all'uniformazione delle condizioni alle quali gli operatori digitali dovranno soggiacere per poter prestare i propri servizi nel mercato interno dell'UE[112].

I due regolamenti appaiono formalmente distinti, occupandosi di materie diverse. Spe-

---

106 In Italia è nota la vicenda che qualche anno fa coinvolse una ragazza, che si era tolta la vita per la vergogna provata per il fatto che per alcuni mesi, senza il suo consenso, erano circolati su *social network* foto e video di intimità sessuali pubblicati su Facebook dal fidanzato. La madre della ragazza aveva proposto ricorso d'urgenza contro la piattaforma sociale, che, nonostante le richieste, non aveva rimosso i post, ottenendo il risarcimento del danno solo tre anni dopo e solo dopo una lunga vicenda giudiziaria (Tribunale di Napoli, sez. II civ., 3 novembre 2016).

107 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 modi- fica le direttive (UE) 2019/1937 e (UE) 2020/1828 (*Digital Market Act*).

108 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 diretti- va 2000/31/CE (*Digital Service Act).*

109 Così anche O. Pollicino, *Regolazione e innovazione tecnologica nell'"ordinamento della Rete",* relazione tenuta al Convegno Nazionale della Associazione Italiana dei Costituzionalisti, *"La libertà di manifestazione del pensiero",* svoltosi a Salerno 15-16 novembre 2024, 40.

110 M.R. Allegri, *Il futuro digitale dell'Unione Europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in *Rivista italiana di informatica e diritto*, 1, 2021, 11 e 12.

111 L. Torchia, *Stato digitale*, cit., 77.

112 M.R. Allegri, *Il futuro digitale dell'Unione Europea,* cit., 10.

cificatamente, il DMA si occupa dei rapporti fra le piattaforme e i fornitori dei servizi, mentre il *Digital Service Act* dei rapporti fra questi ultimi e gli utenti.
Tale distinzione è utile meramente a fini esplicativi, poiché è evidente che nel mercato digitale i momenti di sovrapposizione fra i due tipi di regolazione sono inevitabili, tanto più che le piattaforme sono solo degli intermediari fra i fornitori di servizi e coloro che invece li richiedono.
In realtà essi vanno letti insieme, poiché prevedono ampi e penetranti poteri di vigilanza, controllo e sanzione in capo alla Commissione sulle *Over the Top Companies* (a tal fine indentificate preliminarmente come *Gatekeepers*), cui poi si aggiungono anche quelli degli Stati membri.
Le ragioni che hanno convinto i legislatori europei alla approvazione del DMA sono quelle determinate dalla consapevolezza della insufficienza delle regole *antitrust*, a soccorrere alle nuove esigenze del mercato digitale, poiché sostanzialmente fondate su controlli *ex post* e, quindi, che ad esse debbano necessariamente affiancarsi nuove regole che dispongano anche un quadro di obblighi *ex ante* da imporre a queste imprese, indipendentemente dalla individuazione del mercato rilevante.
Per questi fini il Regolamento stabilisce anche una serie di precisi indicatori sulla base dei quali individuare il prestatore di servizi qualificabile come *Gatekeeper* (art. 3).
In questo modo viene istituito un sistema di presunzione *ex ante* della qualificazione, con la contestuale attribuzione alla Commissione di un ruolo centrale, la quale peraltro vigila sui numerosi e articolati obblighi imposti ai *Gatekeepers* (artt. 5-17), con ampi poteri di indagine, monitoraggio ed esecuzione delle norme del DMA, oltre che di quelli sanzionatori e la capacità di imporre rimedi comportamentali o strutturali.
La disciplina dettata dal *Digital Service Act* (*DSA*), invece, reca regole a protezione degli utenti *online*, per garantire la loro libertà di espressione, ma anche la libertà di iniziativa economica delle piattaforme[113].
La normativa ruota intorno a tre cardini fondamentali: l'individuazione della responsabilità dei *provider*, gli obblighi di diligenza e la cooperazione con le autorità.
Quanto al primo punto, la disciplina, abrogando con l'art. 71 la previgente relativa ai servizi delle società di informazione 2000/31, determina una ridefinizione generale della responsabilità degli intermediari (tra questi ovviamente anche le piattaforme e i *social networks*), che prescinde dalla tipologia del servizio che svolgono, imponendo che la eventuale irresponsabilità del *provider* debba essere provata di volta in volta, divenendo, peraltro, sempre più ardua via via che aumenta la complessità del servizio offerto.
Si determina così una palese rivoluzione copernicana, rispetto al regime precedente, nel quale invece vigeva al contrario la presunzione di neutralità dell'intermediario[114].

[113] Così anche O. Pollicino, *Regolazione e innovazione tecnologica nell'"ordinamento della Rete",* cit., 40, che afferma che scopo della disciplina è «"addomesticare" i giganti del mercato digitale e, quindi, andare direttamente a intervenire su uno degli aspetti caratterizzanti la società algoritmica […] combinando insieme, da un lato, novità concernenti gli obblighi dei *provider* alla tutela di un ambiente digitale trasparente e sicuro e, dall'altro lato, nuove regole relative alla promozione della concorrenza».

[114] Gli artt. 14 e 15 del DSA individuano nella procedura di *notice and take down* il principale strumento di cooperazione fra intermediari e utenti, finalizzato alla rimozione dei contenuti, imponendo alle prime che l'accesso alle notifiche da parte dei secondi sia facile e a che la notifica sia formulata con precisione, in modo da consentire una effettiva conoscenza dell'illecito e all'intermediario di adottare le decisioni conseguenti (art. 14). La eventuale decisione di rimozione del contenuto dovrà essere poi notificata al

Ciò che non viene definito dal DSA è però l'esatta nozione di contenuto illecito, dedicandosi più che altro a dettare norme di carattere procedurale volte alla moderazione e alla eventuale rimozione dello stesso e lasciando tale individuazione alle autorità giudiziarie nazionali (considerando 29 del DSA)[115].

In questo modo, secondo una condivisibile opinione della dottrina, i *providers* per discernere e valutare quali contenuti dovranno necessariamente essere moderati, avranno a disposizione un *corpus* normativo vastissimo sia di livello europeo sia di livello nazionale, che potrebbe facilmente determinare l'insorgere di controversie fra utenti, autorità nazionali e operatori digitali[116].

Un ulteriore aspetto innovativo del DSA è che esso modula e diversifica gli obblighi di cooperazione e vigilanza a seconda delle dimensioni degli intermediari e alla complessità dei servizi da loro offerti, distinguendoli in quattro categorie: *intermediary services, hosting, online platform e le very large online platforms*[117].

A queste ultime è richiesto, come obbligo aggiuntivo di cooperazione, quello di istituire ulteriori meccanismi di gestione dei reclami, che dovranno essere gestiti in modo tempestivo, diligente e obiettivo, come anche le decisioni sui contenuti.

Gli obblighi di moderazione dei contenuti, come anche quelli di controllo, imposti alle *Very Large Platforms* sono quindi ancora più severi. Esse, infatti, sono onerate anche

destinatario con adeguata motivazione, in modo da consentirgli di reclamare la decisione attraverso i meccanismi interni, o di risoluzione extragiudiziale delle controversie o ancora per via giudiziaria (art. 15).

[115] Il considerando 29 dispone infatti che «a secondo dell'ordinamento giuridico di ciascuno Stato membro di ciascuno Stato membro e del settore del diritto in questione, le autorità giudiziarie o amministrative nazionali possono ordinare ai prestatori di servizi intermediari di contrastare determinati contenuti illegali specifici o di fornire determinate informazioni specifiche»

Per discernere ciò che costituisca contenuto illegale, l'interprete deve infatti rifarsi, intanto, al considerato n. 12 che ne fornisce una ampia interpretazione, introducendovi «informazioni, indipendente- mente dalla loro forma, che ai sensi del diritto applicabile sono di per sé illegali [...] A tale riguardo è irrilevante che l'illegalità delle informazioni o delle attività sia sancita dal diritto dell'Unione o dal diritto nazionale conforme al diritto dell'Unione e quale sia la natura esatta o l'oggetto preciso della legge in questione».

A questo si deve anche aggiungere, l'art. 2 lett. g) del DSA, che qualifica "contenuto illegale" «qualsiasi informazione che, di per sé o in relazione ad un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme alle disposizioni normative dell'Unione o di uno Stato membro, indipendentemente dalla natura o dall'oggetto specifico di tali disposizioni».

[116] M.R. Allegri, *Il futuro digitale dell'Unione Europea,* cit., 15.

D'altro canto, non può sorprendere la decisione del legislatore europeo di non disporre in modo sostanziale della definizione di "contenuto illegale", per diversi ordini di ragioni: i citati problemi definitori di ciò che sia *fake news* (e oggi *deepfake*) e disinformazione; il rischio che la cristallizzazione in disposizioni positive di tali definizioni non sarebbe in grado di seguire l'evoluzione tecnologica sottesa alla manifestazione delle opinioni online e renderebbe precocemente obsolete le norme stesse; le limitazioni alla libertà di espressione che da tale definizioni deriverebbero.

[117] Queste ultime sono le piattaforme digitali che hanno in media oltre 45 milioni di utenti attivi mensili nell'Unione europea, pari al 10% della popolazione europea.

A imporre la distinzione sono i considerando da 53 a 63 del DSA. In particolare nel considerando 53 si legge che «Data l'importanza che le piattaforme online di dimensioni molto grandi, per via del loro raggio d'azione, espresso in particolare come numero di destinatari del servizio, rivestono nel facilitare il dibattito pubblico, le operazioni economiche e la diffusione di informazioni, opinioni e idee e nell'influenzare il modo in cui i destinatari ottengono e comunicano informazioni *online*, è necessario imporre a tali piattaforme obblighi specifici, in aggiunta agli obblighi applicabili a tutte le piattaforme online. Tali obblighi supplementari per le piattaforme online di dimensioni molto grandi sono necessari per affrontare tali preoccupazioni di interesse pubblico, in quanto non esistono misure alternative e meno restrittive che consentano di conseguire efficacemente lo stesso risultato».

di valutare i rischi sistemici connessi al funzionamento e all'uso dei loro servizi e ai possibili abusi da parte dei destinatari, con il conseguente obbligo di adottare anche le misure per attenuarli.

La distinzione fra piattaforme e *Very Large Platforms* si coglie anche quanto ai poteri di controllo e di vigilanza. Infatti, per le prime è previsto che in ogni Stato membro si costituiscano appositi organismi di risoluzione extragiudiziale delle controversie fra intermediari e utenti, cui questi ultimi potranno rivolgersi se insoddisfatti dalle scelte delle piattaforme in esito ai reclami o in alternativa rispetto ai reclami stessi.

Inoltre, è previsto che sia individuato presso gli Stati membri anche un coordinatore dei servizi digitali[118], che certifica la sussistenza a livello nazionale di questi organismi e contribuisce alla applicazione coerente del Regolamento. I coordinatori sono inoltre tenuti a cooperare fra loro, con la Commissione e con il comitato europeo per i servizi digitali (art. 18).

Si crea, dunque, quanto al controllo sulle attività delle piattaforme, un sistema reticolare che vede la cooperazione fra i singoli Stati, raccordati in un organismo di livello sovranazionale, e fra questi e la Commissione[119].

La disciplina dei controlli e della vigilanza sulle *Very Large Platforms* è invece del tutto diversa da quella appena descritta per le piattaforme per così dire "ordinarie" e assume una struttura fortemente accentrata.

Esse sono anche soggette, ai sensi degli artt. 50 e ss., ad una procedura di vigilanza rafforzata, relativa alla conformità delle loro attività rispetto alle norme del Regolamento, che coinvolge la Commissione europea. Il ruolo di quest'ultima, infatti, sovrasta quello degli altri organismi di controllo, potendo essa intervenire direttamente di sua iniziativa nel caso di persistenza delle violazioni, svolgendo autonomamente indagini e audizioni, ispezioni in loco, adottando misure provvisorie, rendendo vincolanti impegni e finanche irrogare sanzioni pecuniarie per le violazioni del regolamento (artt. 50-66).

Ciò evidentemente avvicina il modello di controllo delle *Very Large Platforms* a quello *antitrust* e presenta degli importanti punti di collegamento alla disciplina di controllo di cui al *Digital Market Act*, tanto che parte della dottrina lo ha definito "controllo gemello" rispetto a quest'ultimo[120].

---

[118] I poteri dei quali sono disciplinati agli artt. 38, 39 e 41 del DSA.

[119] L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale,* in *Rivista trimestrale di diritto pubblico*, 2022, 1110.
Al sistema di controllo reticolare appena descritto si aggiunge il sistema dei "segnalatori attendibili", di cui all'art. 19 DSA. Si tratta in particolare di enti accreditati dagli Stati membri che rappresentano interessi collettivi e sono indipendenti dagli intermediari digitali, le cui segnalazioni vanno trattate con priorità. Come con analoga priorità le piattaforme potranno reagire sospendendo i servizi nei confronti di quegli utenti che con frequenza diffondono contenuti manifestamente illegali (art. 20, par. 1).

[120] M.R. Allegri, *Il futuro digitale dell'Unione Europea,* cit., 17.

7.2. (*segue*) L'*AI Act* e il disegno di legge italiano sull'Intelligenza Artificiale

Alla normativa dettata dal *Digital Market Package* oggi si aggiunge l'*AI Act*[121] entrato in vigore il 2 agosto 2024, è caratterizzato da termini progressivi di applicazione delle sue disposizioni, che saranno applicabili nella loro totalità a 36 mesi dalla entrata in vigore stessa. Il rischio, a fronte di questa applicazione graduale, è quello del precoce invecchiamento di norme dettate molti mesi prima in una materia che affronta l'inarrestabile evoluzione tecnologica, la quale per sua natura procede ad un ritmo e ad una velocità non contenibile entro confini di natura temporale.

Esso si pone come pietra miliare della disciplina europea in tema di Intelligenza Artificiale, in una società che grazie a questa tecnologia si sta velocemente evolvendo da società digitale a *cybersociety*[122]*,* modificando l'approccio normativo dalla «automazione fondata sull'"algoritmo" a una prospettiva sempre più fondata sull'"intelligenza artificiale"». Laddove, «mentre l'algoritmo si sostanzia in una sequenza di istruzioni ben definite, non ambigue e, dunque, applicate in modo meccanico dalla macchina, l'intelligenza artificiale, fondandosi per lo più su sistemi di *machine learning*, si caratterizza per il fatto di essere in grado di elaborare autonomamente regole di inferenza a partire dai dati usati per l'allenamento»[123].

Fra gli obiettivi principali del Regolamento quello della protezione degli utenti e dei loro diritti fondamentali, imponendo alle piattaforme gestorie obblighi di informazione laddove i singoli interagiscano con tali sistemi (anche e soprattutto con immagini, contenuti audio o video artificiali o manipolati, come nel caso dei *deepfake*) e implementando i controlli sul trattamento e la gestione dei dati personali.

In primo luogo, esaminando il regolamento, va sottolineato come l'ambito di applicazione (art. 2) si estenda ai fornitori che immettono sul mercato o mettono in servizio sistemi di Intelligenza Artificiale nell'Unione, indipendentemente dal fatto che siano stabiliti nell'Unione o in un Paese terzo, nonché agli utenti dei sistemi di IA situati nell'Unione e ai fornitori e agli utenti di sistemi di IA situati in un Paese terzo, ove l'*output* prodotto dal sistema sia utilizzato nell'Unione.

La strategia dell'Unione europea è, dunque, quella di porsi come *leader* nella produzione normativa anche in questo campo, facendo sì che il modello europeo divenga un riferimento globale e possa essere adottato nelle altre regioni del mondo, per esempio con

[121] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale.

[122] Così si esprime O. Pollicino, *Regolazione e innovazione,* cit., 44-45 che cita anche L. Violante, *Diritto e potere nell'era digitale. Cybersociety, cybercommunity, cyberstate, cyberspace: tredici tesi*, in *Biolaw Journal – Rivista di Biodiritto,* 1, 2022, 145 ss. e A. Simoncini - S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 1, 2019, 87–106.

[123] O. Pollicino, *Regolazione e innovazione*, cit*.,* 45. Si veda anche A. Simoncini, *Il linguaggio dell'Intelligenza Artificiale e la tutela costituzionale dei diritti*, in *Rivista AIC*, 2, 2023, 1–39.

gli Stati Uniti[124] (il cosiddetto «effetto Bruxelles»)[125].

Leggendo l'*AI Act* in combinato disposto col GDPR, nonché con il DMA e il DSA, si ha quindi l'idea di un disegno normativo generale nell'Unione europea volto a salvaguardare non solo i diritti di tutti coloro che entrino in contatto con la tecnologia digitale, ma anche i "valori" europei in senso culturale. Infatti, il termine "valori" è menzionato più volte nell'*AI Act*, in modo da «sottolineare che il modello elaborato non è solo normativo, ma culturale. Si vuole rendere evidente che non si tratta soltanto di regole giuridiche, ma anche della cultura che quelle regole esprimono»[126].

L'approccio adottato dal legislatore europeo per la regolazione della Intelligenza Artificiale è stato definito "orizzontale"[127], con norme anche in questo caso estremamente generali di carattere procedurale volte «non a risolvere specifici problemi o a colmare determinate lacune dell'ordinamento, ma applicabili a qualunque settore, […] per delineare un quadro complessivo, un contesto di riferimento nel quale opereranno i sistemi di intelligenza artificiale, anche quelli ancora da venire»[128].

Seguendo, dunque, lo stesso modello adottato per il *Digital Markets Package*, il regolamento muove dalla classificazione delle tecnologie di IA fondata su quattro categorie, in ragione del rischio che presentano: sistemi a rischio inaccettabile, ad alto rischio e a rischio basso o minimo.

I primi, identificati dall'art. 5, sono assolutamente vietati. Per i sistemi di IA a basso rischio, invece, sono previsti alcuni obblighi di trasparenza e si incoraggia l'adozione di codici di condotta (art. 93)[129]. Lo stesso regolamento dispone che per i *deepfake*, considerati anche essi sistemi a basso rischio, a meno che non comportino la commissione di reati, è previsto che gli utenti rendano noto che il contenuto è stato generato o manipolato artificialmente.

Infine, la gran parte del regolamento è dedicata a prevedere in dettaglio gli obblighi per l'adozione di sistemi di IA ad alto rischio[130], che saranno soggetti a determinati vincoli prima di poter essere utilizzati tra i quali l'obbligo di fornire adeguata documentazione contenente tutte le informazioni necessarie sullo scopo del sistema, affinché le autorità possano valutarne la conformità[131], la predisposizione di una valutazione dei rischi, la

---

[124] G. Finocchiaro, *La regolazione,* cit., 1091-1092, afferma che la strategia normativa dell'UE ha un evidente obiettivo geopolitico, volendo contrastare in questo modo la *leadership* tecnologica cinese e statunitense. In particolare, come si è già accennato al § 5, l'approccio statunitense sembra sviluppare un «modello auto-regolatorio basato sull'*antitrust*».

[125] A. Bradford, *The Brussels Effect: How the European Union Rules the World*, New York, 2020.

[126] G. Finocchiaro, *La regolazione,* cit., 1091.

[127] Ivi, 1089.

[128] Ivi*,* 1093.

[129] Ad esempio, per i sistemi di IA destinati a interagire con le persone fisiche, è richiesto che esse siano informate del fatto che stanno interagendo con un sistema di IA; per i sistemi di riconoscimento delle emozioni o di categorizzazione biometrica, è prescritto agli utenti di informare delle loro modalità di funzionamento le persone fisiche che vi siano esposte.

[130] Si tratta di tutte le applicazioni che comprendono sistemi in grado di arrecare danni significativi alla salute, alla sicurezza, ai diritti fondamentali o all'ambiente delle persone, includendovi quelli utilizzati per l'influenzare gli elettori e i risultati delle elezioni ed i sistemi di raccomandazione utilizzati dalle piattaforme dei *social media* con una base utenti superiore a 45 milioni.

[131] Si tratta di una procedura di valutazione della conformità *ex ante*, la quale si conclude con l'apposizione

garanzia sulla tracciabilità dei risultati.

Sebbene l'*AI Act* sia il primo atto normativo che ambisce a regolare per intero questo settore, esso presenta delle indubbie criticità[132].

In primo luogo, la classificazione dei sistemi di IA sulla base del rischio cristallizza oggi una tecnologia in continuo divenire e dunque anche queste tipologie saranno necessariamente soggette a revisione, poiché certamente verranno sviluppati nuovi sistemi e nuovi metodi per implementare quanto già esistente, modificando il livello di rischio.

In secondo luogo, le medesime soluzioni, anche in termini di *accountability*, sono adottate indiscriminatamente per soggetti e ambiti assai diversi fra loro e a prescindere dalle dimensioni delle imprese, profilandosi dunque forti rischi per le imprese di piccole dimensioni e per le *start-up*.

Dal punto di vista sostanziale, infine, pur ponendosi a tutela dei valori europei, il regolamento si limita a vietare i sistemi di intelligenza artificiale che comportano un rischio inaccettabile, rinviando poi, in modo implicito o esplicito, ai principi generali che sono ormai al cuore del diritto europeo (come la dignità, la trasparenza, la protezione dei dati personali), senza prevedere delle specifiche modalità di applicazione degli stessi ai sistemi di intelligenza artificiale, né forme nuove e più efficaci di tutela dell'individuo[133].

Che quello della regolazione sia il modello prescelto in Europa, lo si comprende anche dal fatto che alla luce dell'*AI Act* alcuni Stati stanno promuovendo l'approvazione di proprie normative nazionale sul tema. In Italia, per esempio, presso l'Ottava Commissione (congiunta con la Decima) del Senato della Repubblica si sta svolgendo l'esame in sede referente del disegno di legge n. 1146 di iniziativa governativa intitolato "Disposizioni e delega al Governo in tema di Intelligenza Artificiale"[134].

La proposta di legge mira a definire, nel rispetto dell'*AI Act*, per la cui attuazione viene data delega di adozione di uno o più decreti legislativi, un quadro normativo domestico in relazione ad alcuni aspetti cruciali connessi all'utilizzo dei sistemi di IA, con particolare riferimento a quei settori nei quali tale utilizzo potrebbe avere un impatto significativo a livello sociale ed economico e con l'ambizione di fornire una risposta ad alcune delle preoccupazioni manifestate a proposito dell'utilizzo di IA in settori come la sanità, la Pubblica Amministrazione, la giustizia e le professioni.

L'intento del Governo proponente sembra quello di voler accelerare l'introduzione di alcuni dei principi previsti dall'*AI ACT*, di meglio disciplinare alcune aree potenzialmente critiche interessate dall'utilizzo dei sistemi di IA, consentendo all'Italia di avere una presenza strategica nel contesto europeo.

Per questo motivo, il testo contiene richiami espliciti ai diritti fondamentali ed alle libertà previste dalla Costituzione italiana e dal diritto dell'UE, nonché ai principi di

della marcatura CE (art. 48).

[132] Si veda L. Floridi, *The European Legislation on AI: A Brief Analysis of its Philosophical Approach*, in *Philosophy and Technology*, 2021,, 216 e G. Finocchiaro, *La regolazione,* cit., 1094 ss.

[133] Come, infatti, rilevato da G. Finocchiaro, *La regolazione,* cit., 1098, il regolamento «definisce una cornice di natura amministrativa per l'immissione nel mercato dei prodotti di Intelligenza Artificiale. Il quadro generale dovrà però essere completato dalle norme tecniche e dagli standard, che rivestiranno un'importanza fondamentale, e dovrà essere continuamente aggiornato».

[134] Il disegno di legge di iniziativa del Governo è stato approvato dal Consiglio dei ministri il 23 aprile 2024.

trasparenza, proporzionalità, sicurezza, valorizzazione e protezione dei dati personali, accessibilità e non discriminazione, a presidio dell'autonomia e dell'autodeterminazione umana. Analogamente la definizione di "sistema di intelligenza artificiale" corrisponde esattamente a quella contenuta nel regolamento europeo.

Quanto alla privacy, il testo ribadisce il principio fissato dall'art. 22 del GDPR secondo cui ciascuno ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresi i trattamenti svolti dai sistemi di intelligenza artificiale, sebbene non vengano fornite indicazioni specifiche su come debba essere gestito il trattamento dei dati personali, limitandosi a rimandare alla legislazione corrente.

Limitatamente al tema oggetto di questo lavoro, l'art. 4 del citato disegno di legge nel disporre che «L'utilizzo di sistemi di intelligenza artificiale nell'informazione avviene senza pregiudizio alla libertà e al pluralismo dei mezzi di comunicazione, alla libertà di espressione e […] dell'informazione», garantisce anche «il *trattamento lecito, corretto e trasparente* dei dati personali […] in conformità con il diritto dell'Unione europea in materia di dati personali e di tutela della riservatezza»[135], evidentemente rinviando all'*AI Act*, e, inoltre, rafforza la tutela dei minori disponendo che il loro accesso a tale tecnologia avvenga «consenso di chi esercita la responsabilità genitoriale»[136].

Considerazioni finali

L'analisi dei rimedi posti dal diritto dell'Unione europea (e proposti nell'ordinamento italiano), volti a disciplinare i servizi resi dagli intermediari *online* (i.e. il *Digital Markets Package*) anche per mezzo dell'Intelligenza Artificiale (i.e. *AI Act*) e a porre un argine sul fronte del diritto penale ai reati commessi per mezzo di questa nuova tecnologia, sollecita delle brevissime riflessioni conclusive.

In prima battuta si è avuto modo di rilevare che in assenza di una disciplina positiva era stata la giurisprudenza (in specie si è analizzata quella della Corte di Giustizia dell'Unione europea, ma analoghi rimedi giurisprudenziali sono stati posti al livello dei singoli Stat e della Corte EDU) a porre un argine a tutte quelle situazioni giuridiche lesive dei diritti dei singoli e che sorgono a causa del diffondersi della tecnologia digitale e dei sistemi di IA.

In particolare, si è avuto modo di constatare come nell'Unione europea è facilmente estendibile alle fattispecie di *deepfakes* illegali la giurisprudenza sulla disinformazione e come negli Stati Uniti i giudici dei singoli Stati stiano apprestando analoghe tutele alle vittime, laddove però esistano leggi statali specifiche sul tema.

Va ribadito che in USA la mancanza di una legge federale determina la grave frammentazione dei possibili argini al diffondersi di reati di tal fatta e lascia ai singoli Stati il compito di gestire, autonomamente, l'impatto dell'IA generativa in questioni così delicate[137].

[135] Art. 4, c. I e II.

[136] Art. 4, c. IV, il quale ulteriormente dispone che: «Il minore degli anni diciotto, che abbia compiuto quattordici anni, può esprimere il proprio consenso per il trattamento dei dati personali connessi all'utilizzo di sistemi di intelligenza artificiale, purché le informazioni e le comunicazioni di cui al comma 3 siano facilmente accessibili e comprensibili».

[137] Per completezza si deve segnalare che tuttavia, alcune leggi federali esistenti riguardano l'AI, sebbene con applicazioni limitate. Un esempio è il *National AI Initiative Act* del 2020 (aggiornato, da ultimo, nel

In questo è evidente come l'approccio europeo al tema sia molto diverso da quello statunitense, così come invero accade anche per la tutela della libertà di espressione che si esprime attraverso modelli essenzialmente diversi fra le due sponde dell'Atlantico, avvicinando anche sotto questo aspetto le fattispecie di *fake news* a quelle di *deepfake*, i quali sembrano i "successori" delle prime, progrediti grazie all'evoluzione della tecnologia.
Quello statunitense manifesta oggi una visione del tutto *business friendly* volta a favorire le imprese e a tutelarne lo sviluppo, per mezzo delle sole disposizioni di natura *antitrust* e di una totale deregolazione dello sviluppo delle tecnologie di IA, mirato a garantire in questo modo la *leadership* americana del settore.
L'Unione europea con il DMA, il DSA e l'*AI Act* mostra invece la sua visione "umanocentrica", che pone invece al centro i diritti dei singoli e i valori dell'Unione.
Entrambe le soluzioni però lasciano irrisolto un nodo che accompagna tutte riflessioni rese nel presente lavoro, restando sempre sullo sfondo: la necessità di garantire alle vittime di *deepfake* una tutela effettiva, ma anche rapida, che non aspetti i tempi lunghi della giustizia e che si dimostri adeguata alla velocità con la quale la disinformazione si diffonde nel *web*.
A tal proposito soccorre in aiuto un'idea sviluppata anni fa da certa parte della dottrina italiana[138] in tema di manifestazione del pensiero, che potrebbe validamente essere applicata anche in questi casi, che, come già sostenuto, possono essere considerati una evoluzione del problema delle *fake news*, determinata dallo sviluppo della tecnologia.
La tesi sosteneva che sarebbe stato possibile costruire una rete di controllo di Autorità nazionali, collegate alla Commissione europea, sul modello delle Autorità *antitrust*, in modo che velocemente i *fake* (*fake news*, ma oggi potrebbe dirsi analogamente per i *deepfake*) possano essere valutati come tali e altrettanto velocemente rimossi.
L'idea è stata molto criticata in origine[139], ma oggi ritrova la sua validità se aggiornata e rivalutata in base al nuovo contesto normativo vigente nell'Unione europea (specificatamente il *Digital Market Package* e l'*Artificial Intelligence Act*).
Il primo, infatti, impone alle piattaforme di cooperare con le autorità europee nell'identificare i *fake,* adottando il principio della responsabilità dell'intermediario *online,* e individua nella Commissione europea l'organo deputato al controllo ultimo e centralizzato.
L'*AI Act* poi all'art. 70 espressamente dispone l'istituzione o l'individuazione di Autorità Indipendenti presso i singoli Stati membri, che svolgano l'attività di controllo, notifica e vigilanza in stretta comunicazione con la Commissione[140].

2023), che ha l'obiettivo di ampliare la ricerca e lo sviluppo nel campo dell'AI e ha istituito il *National Artificial Intelligence Initiative Office*, responsabile della supervisione e dell'implementazione della strategia nazionale statunitense sull'AI.

[138] La tesi di G. Pitruzzella resa nota dapprima con due interviste concesse al *Financial Times* il 30 dicembre 2016 *Italy antitrust chief urges EU to help beat fake news* e al *Corriere della Sera* il 2 gennaio 2017 *Quel filtro necessario per le notizie false sul web*, poi ulteriormente sviluppata in Id., *La libertà di informazione*, 82, 93-95.

[139] C.A. Carnevale Maffé, *Neppure l'Autorità della Veridicità può fermare il mercato delle bufale*, in *Il Foglio*, 7 gennaio 2017 e analogamente si vedano C. Melzi D'Eril – G.E. Vigevani, *Difesa giuridica dal sociachiacchiericcio*, in *Il Sole 24 Ore*, 2 aprile 2017; M. Bassini, *Fake news: perché non è un lavoro da spazzini (del web)*, in *medialaws.eu*, 16 marzo 2017; N. Zanon, *Fake News e diffusione dei social media: abbiamo bisogno di un'"Autorità Pubblica della Verità"?*, in questa *Rivista*, 1, 2018, 17.

[140] Art. 70, par. 1, dell'*AI Act* dispone infatti che: «Ciascuno Stato membro istituisce o designa come

Analogamente la proposta di legge italiana sulla IA, in attuazione delle disposizioni del regolamento europeo, pur mantenendo impregiudicate le attribuzioni dell'Autorità Garante per la Protezione dei Dati Personali, individua nell'Agenzia Italiana per il Digitale (AgID) e nell'Agenzia per la Cybersicurezza Nazionale (ACN) le Autorità Nazionali per l'Intelligenza Artificiale, distinguendone i compiti e le funzioni (art. 18).
In particolare, la prima sarà responsabile di promuovere l'innovazione e lo sviluppo dell'Intelligenza Artificiale e di provvedere a definire le procedure e ad esercitare le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale, secondo quanto previsto dalla normativa nazionale e dell'Unione europea. L'ACN, anche ai fini di assicurare la tutela della cybersicurezza, sarà responsabile per la vigilanza, ivi incluse le attività ispettive e sanzionatorie, dei sistemi di intelligenza artificiale, secondo quanto previsto dalla normativa nazionale e dell'Unione europea. Entrambe, invece, per quanto di rispettiva competenza, assicurano l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di intelligenza artificiale conformi alla normativa nazionale e dell'Unione europea.
Da ultimo una considerazione finale, i temi trattati in questo lavoro si pongono al confine fra diritto pubblico e diritto privato, in un momento in cui il potere pubblico sembra riappropriarsi della sua sovranità normativa, che, fino a qualche tempo fa a causa del vuoto normativo persistente in materia, sembrava persa in favore delle grandi piattaforme sovrane del mondo digitale.
Si tratta di un terreno accidentato e per lo più sconosciuto, che pone il quesito di «come edificare il nuovo diritto costituzionale dell'Intelligenza Artificiale tra dimensione pubblica e privata»[141].
A tale quesito si può forse rispondere ritenendo che le prospettive aperte dalla nuova regolazione europea dell'IA devono essere accompagnare necessariamente dalla valorizzazione degli strumenti giuridici esistenti, come la tutela rafforzata dei diritti fondamentali e la garanzia di adeguati e omogenei livelli qualitativi dei servizi indispensabili al soddisfacimento dei diritti fondamentali, che imporrebbero ai proprietari privati dei sistemi di IA un dovere di protezione, divenendo titolari di obblighi tipici dei soggetti pubblici, come la trasparenza e l'imparzialità.
In questo modo il potere (espresso anche da soggetti privati che gestiscono le piattaforme *online*) sarebbe nuovamente catturato e limitato e il costituzionalismo riscoprirebbe la propria primigenia missione[142].

autorità nazionali competenti ai fini del presente regolamento almeno un'autorità di notifica e almeno un'autorità di vigilanza del mercato. Tali autorità nazionali competenti esercitano i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione del presente regolamento. I membri di tali autorità si astengono da qualsiasi atto incompatibile con le loro funzioni. A condizione che siano rispettati detti principi, tali compiti e attività possono essere svolti da una o più autorità designate, conformemente alle esigenze organizzative dello Stato membro».

[141] A. Simoncini, *La dimensione costituzionale dell'Intelligenza Artificiale,* in G. Cerrina Feroni – C. Fontana – E.C. Raffiotta (a cura di), *AI Anthology,* cit., 150.

[142] A. Simoncini, *La dimensione costituzionale,* cit., 154 riprende anche l'idea di M. Luciani, *Costituzionalismo irenico e costituzionalismo polemico*, in *Giurisprudenza costituzionale,* 4, 2006, 1668.

Credit scoring judicial review between the Court of Justice of the European Union and comparative case law*

Elena Falletti, Chiara Gallese

Abstract

Credit scoring is a widespread practice that assigns a score based on certain characteristics or past behaviors, in particular regarding the reliability of debtors to repay loans. In this regard, the new Regulation on Artificial Intelligence (AI Act) adds a control tool to the already well-known art. 22 GDPR, in order to protect consumers and weaker parties, based on which the Court of Justice of the European Union issued the *SCHUFA* decision. However, there are still grey areas in which the balance between the transparency owed to the consumers regarding the processing of their data or the protection of trade secrets in favor of credit score agencies.
This article analyses the orientations of the Court of Justice of the European Union and the national courts regarding credit scoring, following the *SCHUFA* decision, and proposes some reflections on the application of arts. 22 GDPR and 86 AI Act in this context.

Il credit scoring è una pratica diffusa che assegna un punteggio sulla base di alcune caratteristiche o comportamenti passati, in particolare in merito all'affidabilità dei debitori di rimborsare i prestiti ricevuti. A questo proposito, il nuovo regolamento sull'Intelligenza Artificiale (AI Act) aggiunge uno strumento di controllo al già noto art. 22 del GDPR per tutelare i consumatori e le parti deboli, sulla base del quale la Corte di giustizia dell'Unione europea ha emesso la decisione SCHUFA. Tuttavia, esistono ancora aree grigie in cui il bilanciamento tra la trasparenza dovuta ai consumatori in merito al trattamento dei loro dati e la protezione dei segreti commerciali è a favore delle agenzie di credit score.
Questo articolo analizza gli orientamenti della Corte di giustizia dell'Unione europea

*Author contribution: the abstracts and section 1 were written by both authors; Elena Falletti wrote sections 2, 3, and 6; Chiara Gallese wrote sections 4, 5 and 7. This work was partially funded by the European Union, DataCom Project, Grant Agreement no. 101108151. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission and EU executive agencies.
Neither the European Union nor the granting authority can be held responsible for them.
L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

e dei tribunali nazionali in materia di credit scoring a seguito della decisione SCHUFA e propone alcune riflessioni sull'applicazione degli artt. 22 del GDPR e 86 dell'AI Act in questo contesto.

Table of contents

Keywords

Artificial Intelligence – Automated Decision Making – Credit Scoring – Transparency – Comparative Law

1. Introduction

Credit scoring is a statistical method used by banks, other financial institutions, and international agencies to assess the creditworthiness of individuals or businesses applying for credit. Those actors evaluate several financial and non-financial factors to determine the likelihood that a borrower will repay their debt obligations on time. Credit rating agencies played a crucial role in the 2007-2008 crisis by assigning overly optimistic ratings to complex financial instruments, such as subprime mortgages[1]. These inflated ratings gave investors a false sense of security, leading to excessive risk-taking and ultimately contributing to the collapse of the housing bubble and the worldwide crisis[2].

However, such tools can have several negative effects on individuals, that are particularly pronounced for certain demographic groups[3], and can have long-lasting consequences on financial well-being. For example, Consumers who experience a credit rating downgrade, even due to factors beyond their control, may face reduced access to financing for extended periods[4].

Automation and algorithm-driven decision-making systems have transformed the consumer finance industry. What once relied heavily on human judgment has increas-

[1] Z. Guo, *The 2008 Financial Crisis: Causes, Consequences, and Responses* in *Highlights in Business,* in *Economics and Management*, 27, 2024, 373 ss.; A. Astakhova-S Grishunin-G. Pomortsev, *Developing a Scoring Credit Model Based on the Methodology ofInternational Credit Rating Agencies,* in *Journal of Corporate Finance Research*, 2023, 17(1), ss., doi.org/10.17323/j.jcfr.2073-0438.17.1.2023.5-16.

[2] *Ibidem.*

[3] L. Blattner-S. Nelson, *How costly is noise? Data and disparities in consumer credit*, in *arXiv preprint,* arXiv:2105.07554, 2021.

[4] J. M. Garmaise-G. Natividad, *Slippery Slope or Wake-up Call? Negative Credit Rating Shocks for Consumers*, in UCLA Working Paper, 2016.

ingly been shifted to data-driven processes, fueled by large amounts of personal and financial data ("big data"). The rise of AI credit scoring systems, and more recently, "credit analytics" has increased in recent years. However, while automation promises efficiency and objectivity, it often introduces new forms of opacity and discrimination that are largely invisible and hard to challenge. As noted by Pasquale[5], it is not uncommon for consumers to learn that their poor credit score has cost them tens of thousands of dollars over the course of a mortgage or other long-term loans. Yet, how these scores are calculated remains largely a mystery, hidden behind proprietary algorithms and trade secrets that are not open to public scrutiny[6]. While there are general guidelines on what factors influence a credit score (such as payment history, amounts owed, and length of credit history) the precise formula is unknown[7]. This secrecy causes consumers several troubles, as they are unable to fully understand the basis on which their financial credibility is judged[8].

Furthermore, there is the additional problem of relevance, accuracy, and timeliness of data, which are all indicators of data quality. As known, the quality of data influences the results of any analysis, whether it is based on AI or not, as it is impossible to produce an accurate output from inaccurate data. Therefore, data subjects who are the object of such analysis have a strong interest in credit-scoring players keeping their data as accurate as possible to avoid unfair decisions.

However, due to the opacity of these systems, it is impossible to know how, when, and how often credit-scoring agencies update personal data in their databases. Without proper transparency measures, it is very difficult for data subjects to exercise their right to correct their data according to GDPR, as in order to do so it is necessary to know that an error exists in the first place. For example, it is often the case that consumer discovers after many months or even years that their name has been wrongly connected to insolvency cases due to identity theft, and this causes a significant amount of trouble, starting from the impossibility of accessing credit.

If the prison for debt no longer has metal bars as it did for Little Dorrit and her family[9], the (bad) reputation of debt still has significant consequences that can bog down the existential path of the debtor and by extension, of his family imprisoned by more intangible, but no less effective constraints such as databases of "bad payers"[10] and credit scoring algorithms[11].

---

5 F. Pasquale, *The Credit Scoring Conundrum*, in *U of Maryland Legal Studies Research Paper,* 2013, 2013-45.

6 *Ibidem*.

7 *Ibidem*.

8 *Ibidem*.

9 C. Dickens, *Little Dorrit, Povertry,* London, 1857.

10 R. Muñoz-Cancino-C. Bravo–S. A. Ríos–M. Graña, *On the dynamics of credit history and social interaction features, and their impact on creditworthiness assessment performance,* in *Expert Systems with Applications,* 2023, 2018, 119599; M. S. Moghe–S. Johri, *The Role of Credit Scoring in Modern Banking–An Overview of Methodology & Implementation*, in *UNNAYAN*, XVI, 2024, 209 ss.

11 X. Zhang - L.Yu. *Consumer credit risk assessment: A review from the state-of-the-art classification algorithms, data traits, and learning methods*, in *Expert Systems with Applications* 237, 2024, 121484; A. Bhattacharya, - S. K. Biswas, - A. Mandal, *Credit risk evaluation: a comprehensive study*, in *Multimedia Tools and Applications* 82, 12, 2023, 18217 ss.

What seems objectionable about such systems is that they collect data on both significant defaults (e.g., mortgage payments) and smaller defaults (e.g., missed bill payments), as well as information on personal lifestyles through web scraping of information posted online[12].

From one's "onlife"[13]", an endless multitude of information emerges, forming "fingerprints"[14], that can be used by credit scoring algorithms to better focus both the creditworthiness and the lifestyle and even the personality of the person who is getting into debt.

Credit scoring programs are a subset of predictive software that falls under the umbrella of social scoring[15]. These programs, which generally assess financial reliability, are part of a category of software that evaluates individuals' adherence to socially acceptable behaviors within a community[16].

Social scoring aims to measure an individual's reliability in all aspects, integrating whatever data can be collected on a subject into the calculation[17]. Applying such a concept to the possible predictability of repayment of the loan or mortgage obtained, it is a score developed through a statistical procedure. This procedure quantifies the probability of a person's future solvency based on a combination of the payments made in the past by the same person and their classification within a category of similar subjects, according to their individual characteristics[18].

It's important to note that the starting point for machine learning in credit scoring combines past factors and the social category to which the individual belongs, deduced from their personal characteristics. These characteristics play a meaningful role in the social scoring process. This individual may wish to exercise the fundamental right to be forgotten[19], especially in a sensitive area like insolvency. On this point, the

---

[12] L. Crosato-J. Domenech–C. Liberati, *Websites' data: a new asset for enhancing credit risk modeling*, in *Annals of Operations Research*, 342, 2024, 1671 ss.

[13] L. Gambacorta-Y. Huang-H. Qiu-J.I Wang, *How do machine learning and non-traditional data affect credit scoring? New evidence from a Chinese fintech firm*, in *Journal of Financial Stability*, 73, 2024, 101284.

[14] L. Floridi, *The Onlife Manifesto Being Human in a Hyperconnected Era*, Cham, 2015, *passim*.

[15] C. Loeffflad-J. Grossklags, *How the Types of Consequences in Social Scoring Systems Shape People's Perceptions and Behavioral Reactions*, in *The 2024 ACM Conference on Fairness, Accountability, and Transparency*, 2024, 1515-1530; K. Crawford, *Atlas of AI*, New Haven – London, 2021, 205 ss.

[16] W. Rabe-G. Kostka, *Perceptions of social credit systems in Southeast Asia: An external technology acceptance model*, in *Global Policy*, 2024; G. Cerrina Feroni, *Intelligenza artificiale e sistemi di "scoring" sociale. Tra distopia e realtà*, in *Diritto dell'informazione e dell'informatica*, 1, 2023, 1 ss.

[17] G. Gigerenzer, *Perché l'intelligenza umana batte ancora gli algoritmi*, Milano, 2023, 201.

[18] M. Pincovsky-A. Falcão-W. N. Nunes-A. Paula Furtado-R. C. L. V. Cunha, *Machine Learning applied to credit analysis: a Systematic Literature Review,* in *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*, Chaves, Portugal, 2021, 1-5, doi: 10.23919/CISTI52073.2021.9476350; M. Bücker, et al., *Transparency, auditability, and explainability of machine learning models in credit scoring*, in *Journal of the Operational Research Society* 73.1, 2022, 70 ss.

[19] CJEU, C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014). See A. Palmieri-R. Pardolesi, *Diritto all'oblio: il futuro dietro le spalle*, in *Il Foro Italiano*, 6, 2014, 317 ss; C. Wolf, *Impact of the CJEU's Right to Be Forgotten: Decision on Search Engines and other Service Providers in Europe: Case C-131/12 Google v. Agencia Española de Protectión de Datos (AEPO) and Mario Costeja Gonzalez, Judgment of 13 May 2014*, in *Maastricht Journal of European and Comparative Law,* 3, 2014, 547 ss.; S. Shuntich, *The Life, the Death, and the long-Awaited Resurrection of Privacy* in *Human Rights*, 4, 2014, 2.

debtor needs to be aware of what information referable to him is used in the profiling programs and thus have access to meaningful information on both the authenticity of the data and the logic used in the credit scoring process.
The credit scoring software formalizes an evaluation that, unfortunately, is not free from potential group or classist bias[20], based on one's (potentially outdated) reputation.
This article is developed as follows: first, the litigation that has taken place and is pending before the Court of Justice is analysed, then the remedies that can be used against automated decisions, i.e., art. 22 GDPR and art. 68 AI Act, are compared, then the precedents after the *SCHUFA* decision are discussed, and finally some summary conclusions are outlined.

2. The *SCHUFA* decision by the Court of Justice of the European Union

SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) is a private German company that plays a crucial role in the country's credit reporting and financial services sector. Its primary purpose is to collect, store, and provide information about individuals' and businesses' creditworthiness. This information helps banks, businesses, and other entities make informed decisions about lending money, extending credit, or entering into contracts[21].
The *SCHUFA* case involves an individual who was denied a loan based on a negative credit score provided by SCHUFA to their financial institution. The applicant, suspecting inaccuracies, approached SCHUFA to request information regarding the data stored about them and to challenge the accuracy of their credit score. They also demanded a detailed explanation of how SCHUFA calculated their credit score, as well as the significance and possible consequences of such processing, citing art. 15(1)(h) of the General Data Protection Regulation (GDPR). However, SCHUFA responded by giving the applicant only the credit score and a vague description of its calculation methodology, but not on what specific information was included in the mathematical operation and how it was weighted, arguing that providing a detailed explanation of the scoring process was not possible since it would infringe on its commercial secrecy[22]. SCHUFA also claimed that its obligations under the GDPR were limited because it only provided information to third parties, like banks, and did not make the final decisions directly, such as approving or denying loans.

[20] O. B. Deho-L. Liu-J. Li-J. Liu-C. Zhan-S. Joksimovic, *When the past!= the future: Assessing the Impact of Dataset Drift on the Fairness of Learning Analytics Models*, in *IEEE Transactions on Learning Technologies,* 2024; A. Castelnuovo et al., *Befair: Addressing fairness in the banking sector*, in *2020 IEEE International Conference on Big Data (Big Data)*, IEEE, 2020, 3653; S. Verma-J. Rubin, *Fairness definition explained*, in *2018 IEEE/ACM International Workshop on Software Fairness (FairWare)*, IEEE, 2018, 1 ss.

[21] A. Asymina, *Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring)* in the *Labour Context, Industrial Law Journal*, 2024, dwae035, /doi.org/10.1093/indlaw/dwae035.

[22] This is a matter of litigation pending before the Court of Justice, which will be dealt with in the next paragraph.

This case brings into focus key questions about transparency in automated decision-making under the GDPR, particularly how much information credit scoring agencies like SCHUFA must disclose about their algorithms. It also touches on the balance between individuals' rights to understand how their personal data is processed and companies' rights to protect trade secrets.

After the refusal, the client escalated their complaint against SCHUFA to the Hessian Commissioner for Data Protection and Freedom of Information (HBDI), i.e. the German national data protection authority. The applicant requested the HBDI to compel SCHUFA to reveal the specific logic behind their credit score calculation, as well as the significance and potential consequences of the data processing, invoking their rights under the GDPR. However, the HBDI declined to take action against SCHUFA for two years, eventually dismissing the complaint. The authority justified the credit scoring company as complying with Section 31 of the Federal Data Protection Act (BDSG)[23], requirements, which contains detailed rules on scoring procedure and creditworthiness information.

The client contested this ruling before the Amtsgericht Wiesbaden, the ordinary court, which then sought clarification from the Court of Justice of the European Union. The referring court was grappling with the question of whether art. 22(1) GDPR applied to the automated procedure for determining the probability of default rate. This was a crucial issue, as art. 22(1) of GDPR is designed to protect (natural) persons from the discriminatory risks of purely automated decisions. The main question was whether SCHUFA's credit score, which was essentially a probability value derived from profiling, could be considered an automated decision that significantly impacts individuals when relied upon by a third party, like a bank, to make decisions about

[23] §31 BDSG entitled: "*Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften*". In addition to the controversy that occurred before the VG Wiesbaden, there is extensive case law applying this rule in the German legal system. Among the most significant rulings are (source: *dejure.org*): LG Frankfurt/Main, 26/05/2023 - 24 O 156/21 concerning the illegal reporting of electricity supply contract customers to SCHUFA; LG Mainz, 12/11/2021 - 3 O 12/20, regarding liability for illegal reporting; OLG Naumburg, 10/03/2021 - 5 U 182/20, on credit card contractual conditions; LG Frankenthal, 28/06/2022 - 8 O 163/22, for reporting to SCHUFA despite a dispute; VG Wiesbaden, 27/09/2021 - 6 K 549/21, on the right to erasure for illegal reporting to SCHUFA; KG (Kammergericht), 30/07/2019 - 4 U 90/19 on the revocation of negative registrations made with SCHUFA; LG Lüneburg, 14/07/2020 - 9 O 145/19 on the legitimacy of the interest in data transmission for a small current account overdraft; LG Hannover, 14/02/2022 - 13 O 129/21, on compensation for unauthorized reporting to SCHUFA; OLG Brandenburg, 03/07/2023 - 1 U 8/22, cited on the adequacy of the data retention period (3 years) by the credit agency; OLG Koblenz, 18/05/2022 - 5 U 2141/21 and LG Bonn, 23/10/2019 - 1 O 322/19, both concerning requests for data related to a mobile phone contract; LG München I, 25/04/2023 - 33 O 5976/22, on the transmission of personal data by a telephone company to SCHUFA; OLG Düsseldorf, 11/01/2022 - 16 U 130/21, on asserting the right to informational self-determination in the credit sector; LG Karlsruhe, 02/08/2019 - 8 O 26/19, denial of the applicability of art. 82 GDPR following the processing of a negative score by SCHUFA; OLG Frankfurt, 15/03/2023 - 17 U 134/22, liability for incorrect registration with SCHUFA; LG Arnsberg, 16/06/2020 - 1 O 44/20 on SCHUFA's duty to delete negative information; VG Wiesbaden, 07/06/2021 - 6 K 307/20, regarding the registration of debtors' negative data; LG Osnabrück, 29/04/2020 - 18 O 400/19, concerning insolvency threats; OLG Schleswig, 03/06/2022 - 17 U 5/22, on the registration of a planned insolvency procedure, VG Wiesbaden, 24/09/2021 - 6 K 442/21, on the legitimacy of the supervisory authority's intervention; LG Hamburg, 23/07/2020 - 334 O 161/19, on the conditions for the existence of the right to data erasure after debt extinction; OLG Koblenz, 25/03/2020 - 12 U 2228/19, on the right of rectification of the debtor served with an injunction.

loans or other contracts. The main query was at which stage of the creditworthiness assessment the automated calculation procedure came into play: (a) at the assessment stage, based on data provided by third parties (e.g., the bank) to SCHUFA; (b) in the actual calculation phase.

The CJEU was asked to determine if the mere issuance of a credit score (probability value) by SCHUFA qualifies as such a decision, given that a third party (like a bank) relies on it in making an official, impactful decision—such as denying a loan, which has clear legal and financial consequences. The core legal question is whether the credit score itself, issued by SCHUFA in the first place, can be considered a "decision" under art. 22(1) of the GDPR. Art. 22(1) provides that individuals have the right not to be subject to decisions based solely on automated processing, including profiling, if those decisions produce legal effects or similarly significant impacts on them.

The CJUE first stated that the application of art. 22 GDPR must consider both the wording and the context, objectives, and purposes that an automated decision pursues[24], as well as the fact that the decision does not contain human intervention[25]. Three conditions must coexist for the applicability of art. 22, namely: a) that a decision is necessary[26]; b) that it must be «based solely on automated processing, including profiling», and c) that it must produce «legal effects [concerning the data subject]» or affect «his or her person in a similarly significant way».

As regards point (a), the definition provided in recital 71, according to which, in order to be such, a decision must involve the assessment of the personal aspects of a data subject, who has a right to opt out of that decision if it «significantly» affects their person. In other words, the data subject is entitled to evade the legal effects produced by a purely automated decision affecting them, as in the case of the automated rejection of an online credit application or online recruiting practices managed by algorithms[27].

[24] CJEU, C-579/21, *Pankki* S. (2023), EU:C:2023:501, § 38.

[25] P. Hacker–J. Cordes–J. Rochon, *Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond* in *European Journal of Risk Regulation* 15, 1, 2024, 49 ss.

[26] Under this point, the Advocate General Pikamäe affirmed that «On these points, the Court of Justice aligns with the conclusions of the Advocate General, according to whom "(T)he absence of a legal definition (of decision) indicates that the EU legislature opted for a broad concept which can include a number of acts capable of affecting the data subject in many ways". In this sense, «a "decision" within the meaning of Article 22(1) of the GDPR can either have "legal effects" or "similarly" affect the data subject, which means that the "decision" in question may have an impact that is not necessarily legal but rather economic and social. Since Article 22(1) of the GDPR seeks to protect natural persons against the potentially discriminatory and unfair effects of automated processing of data, it seems that particular vigilance is required and must also be reflected in the interpretation of that provision» (Opinion of the Advocate General Pikamäe, Case C-634/21, 16 March 2023).

[27] S. Ochmann et al., *Perceived algorithmic fairness: An empirical study of transparency and anthropomorphism in algorithmic recruiting*, in *Information Systems Journal,* 34, 2024, 384 ss.; D. Narayanan-M. Mahak–McGuire–S. Schweitzer-D. De Cremer, *Fairness perceptions of artificial intelligence: A review and path forward,* in *International Journal of Human–Computer Interaction* 40, 2024, 4 ss. Recital 71 reads: «The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes "profiling" that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning

The decision referenced aligns with art. 22(1) of GDPR applied to credit scoring activities like those conducted by SCHUFA. Such activities qualify as profiling under art. 4(4) of GDPR due to their automated nature and the inclusion of several personal data. Profiling inherently raises concerns about potential discriminatory outcomes as it involves processing data that might reflect intimate personal aspects, such as health, preferences, interests, economic stability, reliability, location or movements of a particular individual[28].

Under the GDPR framework, such profiling activities are assessed to ensure compliance with fundamental rights. When automated decisions significantly impact individuals (e.g., affecting creditworthiness), art. 22 establishes safeguards, mandating explicit consent or legal necessity and providing the right to contest automated outcomes. The critical balancing required here evaluates the proportionality and necessity of profiling against the backdrop of the data subject's fundamental rights and freedoms.

Indeed, according to recital 71, the specific risks may jeopardise the legitimate interests and rights of the data subject, in particular by taking into account the potential discriminatory effects against natural persons on the grounds of racial or ethnic origin, political opinions, religion or beliefs, trade union membership, genetic status, health or sexual orientation.

Therefore, again according to that recital, appropriate safeguards must be provided and fair and transparent processing must be ensured with due regard for the data subject, in particular by using appropriate mathematical or statistical procedures for profiling and by applying appropriate technical and organisational measures to minimise the risk of errors[29].

---

the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child. In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions».

[28] E. Gil González-P. Paul De Hert, *Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles*, in *Era Forum,* 19, Berlin/Heidelberg, 2019, 597 ss.

[29] S. Wachter - B. Mittelstadt - L. Floridi, *Why a right to explanation of automated decision-making does not exist in the general data protection regulation*, in *International Data Privacy Law* 7.2, 2017, 76 ss.

It is worth noting that recitals, while not part of the operative provisions of specific legislation, are nonetheless incorporated into regulations[30], typically found in the preamble of legal documents such as EU regulations or international treaties to explain the purpose, objectives, and context of the law.

Although recitals do not create enforceable rights or obligations[31], they serve as tools for an "authentic interpretation" by providing insights into the drafter's intent[32]. Courts and legal practitioners often use recitals to resolve ambiguities within the operative provisions, aligning the application of the law with its intended purpose. This interpretive role gives recitals a *de facto* legal effect, reinforcing their importance for understanding and applying legislation. For these reasons, recital 71 is an important instrument to clarify GDPR's provisions.

That being said, the question referred for a preliminary ruling related explicitly to the automated calculation of a probability rate based on personal data concerning a person and their ability to honour a loan in the future. Such a decision produces significant legal effects on the person since the action of the client of the credit scoring company (i.e., the "third party") - to whom the probability result is transmitted - will suffer decisive legal effects, in the sense that an insufficient probability rate will, in almost all cases, lead to a refusal to grant the requested loan[33].

Under this perspective, the calculation of such a rate must therefore be qualified as a decision that produces with respect to a data subject's legal effects concerning them or similarly significantly affects them within the meaning of art. 22(2) GDPR. The latter gives the data subject the "right" not to be subject to a decision based solely on automated processing, including profiling. This provision enshrines a prohibition in principle, the violation of which does not need to be asserted individually by such a person.

---

[30] The legal doctrine has long discussed the legal value of recitals. Klimas and Vaiciukaite were puzzled by the extensive use of these instruments in European law: «it is claimed that while EC recitals have no legal value and cannot be the cause of derogation from an operative provision, they nevertheless create legitimate expectations (such as would defeat an operative provision). This is also strange. Recitals are supposed to be general statements. General statements are not something which ordinarily are recognized as giving rise to legitimate expectations. But also recitals in general (for instance, in contract law) are, well, recitals, not operative provisions and it is hard to fathom how they could give rise to positive obligations or defeat operative clauses. Thus, the doctrine surrounding recitals in EC law is mystifying. It is either irrational or so complicated as to amount to the same thing.». T. Klimas-J. Vaiciukaite, *The law of recitals in European Community legislation*, in *ILSA Journal of International & Comparative Law*, 15, 2008, 61 ss.

[31] In fact, the CJEU has affirmed multiple times that recitals cannot directly create rights and duties, see Case C-136/04, *Deutsches Milch-Kontor v Hauptzollamt Hamburg-Jonas*, EU:C:2005:716; Case C-134/08, *Hauptzollamt Bremen v J. E. Tyson Parketthandel*, EU:C:2009:229. M. den Heijer-T. van Os van den Abeelen-A. Maslyka, *On the use and misuse of recitals in European union law*, in *Amsterdam Law School Research Paper*, 3, 2019.

[32] According to Humphreys et al., recitals are important as the European Court of Justice makes frequent references to them as a support tool to establish the purpose of normative provisions. L. Humphreys-C. Santos-L. Di Caro-G. Boella-L. Van Der Torre-L. Robaldo, *Mapping recitals to normative provisions in EU legislation to assist legal interpretation*, in *Legal Knowledge and Information Systems*, 2015, IOS Press, 41 ss.

[33] S. Bastigkeit Ericstam, *AI in the Workplace: Regulating Explainability and Consent in Algorithmic Management,* in K. Prifti-E. Demir-J. Krämer-K.Heine-E.Stamhuis (eds), *Digital Governance. Information Technology and Law Series*, The Hague, 2024.

As follows from the combined provisions of art. 22(2) of the GDPR and recital 71[34] of that regulation, the Court of Justice stated that the adoption of a decision based solely on automated processing is authorised only in the cases referred to in the aforementioned article, i.e., where such a decision is necessary for the conclusion or performance of a contract between the data subject and a data controller within the meaning of point (a), or where it is authorised by the law of the Union or of the Member State to which the data controller is subject under point (b), or is based on the data subject's explicit consent under point (c)[35].

On this last point, some scholars suggested to pay attention to this point, since the debtor's consent may be given without being aware of it, for example, by signing forms or documents that the applicant signs without due care, either because they are vulnerable[36] or because of a tendency to underestimate the consequences of such an act, or the necessity of the signature to continue with the credit application which, in the applicant's belief, they hope will be successful.

In the cases referred to in art. 22(2)(a) and (c) of that Regulation, the data controller shall implement at least the data subject's right to obtain human intervention, to express their opinion, and to contest the decision. What is more, in the case of the adoption of a decision based solely on automated processing, such as that referred to in art. 22(1) of the GDPR, on the one hand, the data controller is subject to additional information obligations under art. 13(2)(f) and art. 14(2)(g) of that Regulation. On the other hand, the data subject enjoys, by art. 15(1)(h) GDPR, the right to obtain from the data controller, inter alia, «meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject[37]».

The aforementioned information and the data subject's access rights are consistent with the recognition of the right to an explanation and thus with the purpose pursued by art. 22 of the GDPR. It is to protect individuals against risks to their rights and freedoms arising from the automated processing of personal data, such as profiling[38]. Stressing the purpose of art. 22 invokes a sense of protection for the data subjects.

On the other hand, according to the author, in circumstances such as the present case, in which three parties with different interests are involved, namely the profiled applicant, the profiling agency, and the bank granting the loan, if the restrictive interpretation of art. 22 GDPR were to be accepted, there would be a risk of circumvention of art. 22 GDPR itself and, consequently, a gap in the legal protection of the weaker party, namely the person subjected to automated processing. The restrictive interpretation considers the calculation of the probability rate only as a preparatory

[34] G. De Gregorio–S. Demková, *The constitutional right to an effective remedy in the digital age: a perspective from Europe,* in C. van Oirsouw-J. de Poorter-I. Leijten-G. van der Schyff-M. Stremler-M. De Visser (eds), *European Yearbook of Constitutional Law 2023,* The Hague, 2024, 223 ss.

[35] CJEU, C-634/21, *SCHUFA* (2023), § 53.

[36] M. Girolami, *La scelta negoziale nella protezione degli adulti vulnerabili: spunti dalla recente riforma tedesca*, in *Rivista di Diritto Civile*, 2023, 854 ss; S. Kirwan, *Between a knock at the door and a knock to your score: re-thinking 'governing through debt'through the hopeful 'imaginaries' of UK debtors*, in *Journal of cultural economy* 14, 2021, 159 ss.

[37] CJEU, C-634/21, *SCHUFA* (2023), § 56.

[38] CJEU, C-634/21, *SCHUFA* (2023), § 52.

act, whereas only the act adopted by the third party can, i.e., the credit institution, be qualified as a "decision" within the meaning of art. 22(1) GDPR.
On the contrary, in the author opinion, what is assumed is only adherent to what happens during the automated decision-making process, where the mathematical calculation of probability is decisive for the definitive result on creditworthiness, which the applicant credit institution may use to grant money or not.
Even if this were not the case, the person subject to the profiling activity would not be able to access the information to defend themselves since the information is not in the bank's possession but is owned by the company that collects the information and processes it to obtain the result. On the other hand, in light of the statistical calculation being an integral part of the automated decision, there would be a correct attribution of liability on the part of the profiling agency: on the one hand, it is liable to the applicant by the unlawful processing of the data under art. 82 GDPR[39], while from a contractual point of view, it is liable for the relationship with the bank requesting the service of calculating the probability of fulfillment rate.
According to the author, even following a different argumentative logic, in the light of recital 71 of the GDPR, the same conclusion is reached: the data controller, i.e., the profiling agency, must use mathematical or statistical procedures suitable for profiling. It is also obliged to take appropriate technical and organisational measures to correct any errors or biases in the information used to ensure the security of personal data. These measures must consider the potential risks to the interests and fundamental rights of the individual concerned and prevent discriminatory effects against them[40].
It is up to the Verwaltungsgericht Wiesbaden to verify the terms under which art. 31 BDSG is consistent with art. 22 GDPR regarding the adoption of a decision based exclusively on automated processing on the basis of the interpretation developed by the Court of Justice[41].
Thus, according to art. 22(1) GDPR, «the automated calculation by a company providing business information of a probability rate based on personal data relating to a person and concerning that person's ability to meet payment commitments in the future constitutes an "automated decision-making process concerning natural persons" within the meaning of that provision, if the conclusion, performance or termination of a contractual relationship with that person by a third party, to whom that probability rate is disclosed, depends decisively on that probability rate»[42].

[39] A. B. Menezes Cordeiro, *Civil liability for processing of personal data in the GDPR*, in *European Data Protection Law Review*, 5, 2019, 492; R. Strugala, *Art. 82 GDPR: strict liability or liability based on fault?,* in *European Journal Privacy Law and Technologies*, 2020, 71; E. Tosi, Unlawful Data Processing Prevention and Strict Liability Regime Under EU GDPR, in The Italian Law Journal, 2021, 874 ss.

[40] According to K. Lagenbucher, «there is a fundamental tension between the [AI Act] Proposal's policy goal to protect fundamental human rights and its risk-based philosophy». K. Langenbucher-P. Corcoran, *Responsible AI Credit Scoring–A Lesson from Upstart.Com*, in *Digital Finance in Europe: Law, Regulation, and Governance. De Gruyter*, 2022; see also K. Langenbucher, *Responsible AI-based credit scoring–a legal framework*, in *European Business Law Review*, 31.4,2020.

[41] A. Aza, *Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context* in *Industrial Law Journal*, 53, 2024, 840 ss.

[42] CJEU, C-634/21, *SCHUFA* (2023).

3. Advocate General De La Tour's conclusions in the CK case on the relationship between access to information and protection of trade secrets

Another interesting case worth commenting is the CK case[43], which concerned a person who was denied the conclusion or an extension of the contract period by a mobile phone company, regarding a monthly payment of a mere EUR 10 (ten) sum, on the justification that the consumer lacked sufficient financial capacity. The plaintiff's alleged insufficient solvency was determined based on an automated credit assessment by the credit rating company, which was positive. In this litigation narrative there is a further disturbing aspect: this daily life case regards a small amount of the contract for which a credit rating was requested about the continuous payment of a very small sum. As a first consideration, one might ask whether a credit scoring procedure can be imposed for a derisory transaction and whether this entails an imbalance between securing creditworthiness and aggravating the stigma towards the less fortunate and those in serious financial difficulty. In addition, owning a mobile phone line is nowadays an essential service, as it was a landline in past years. Considering the small number of mobile companies, we might wonder what would happen if neither of them were willing to enter into a contract with the same individual based on this kind of assessment: would this person be completely cut off from communications?

While this consideration may concern the social aspects of credit scoring, the repercussions of a legal nature are addressed here. In this regard, art. 15(1)(h) gives the data subject the right to access information concerning him to verify that it is meaningful, accurate, and true. The referring court expressed suspicion about the authenticity of that information, because although the information provided to the applicant attributed to her high creditworthiness, her profiling indicated that she was insolvent even in her financial capacity to pay a sum of at least EUR 10. There is thus a contradiction between, on the one hand, the information provided to the consumer about her data processed and the logic used in the automatic assessment carried out and, on the other hand, the conclusion that the telephone operator drew from the rating assigned.

Therefore, a further critical issue arises: the possibility of legal protection for the logic employed in the credit scoring program by intellectual property rules such as trade secrets. But what does that logic consist of? According to the plaintiff, it would include the personal data of the data subject processed in the context of determining the factors, how this was done, and whether these data were weighed. Together with these must be included the essential parts of the algorithm on which the automated decision-making process is based, including the mathematical formula into which they can be entered, the steps by which that formula leads to that rating, and the understandable explanation of all the values used in that formula, in particular those which are not directly taken from stored information relating to the data subject. Additionally, relevant information shall be included to establish the correlation between the information processed and the valuation made, including an indication and

[43] Opinion of Advocate General De La Tour, Case C-203/22, *CK, Dun & Bradstreet Austria GmbH, Magistrat der Stadt Wien,* 12 September 2024.

adequate description of the valuation functions of all values used in such formula, an explanation of the information necessary to establish the correlation between the information and the valuation in the case of periodic valuations, and a presentation of the index functions used.

The other party invoked the existence of a trade secret under art. 2 part 1 of Directive 2916/943 to protect the algorithm and deny access to the logic used in the automated decision-making process[44].

In this dispute, the referring court observes that invoking industrial secrecy would make access to the information provided for by art. 15 GDPR impossible. Industrial secrets protection would prevent verifying information accuracy and comprehensibility and exercising rights under art. 22(3) GDPR and art. 47 of the Charter of Fundamental Rights of the European Union.

Thus, there would be a conflict between the right of access under art. 15, the right of explanation under art. 22 GDPR, and the right of third parties to the protection of algorithmic processes and the related black box.

The decision in this case could have important legal consequences beyond the specific ruling. It would complement the SCHUFA precedent of the Court of Justice of the European Union on a relevant issue, namely what is meant by «significant information about the logic used» in the context of an automated decision-making process using a black box in relation to the protection of trade secrets about the conduct of the decision-making process itself and thus the logic used.

According to the Advocate General, "significant information" within the meaning of art. 15(1)(h) GDPR must not only be clear and accessible but also accompanied by explanations that enable it to be understood. It is all truer when providing the data subject with information in a highly technical field, such as the interpretability of credit scoring systems. In that sense, such a provision offers the data subject a genuine right to obtain explanations as to the operation of the mechanism underlying an automated decision-making process to which that data subject was subject and the result to which that decision led. Recital 71 GDPR explicitly provides that an explanation of the decision must be issued following such an assessment.

In addition, the data subject must be able to verify the accuracy of the personal data concerning them and of the information concerning the logic used within the framework of an automated decision-making process. Furthermore, they must have the possibility of verifying that there is coherence and an objectively verifiable causal link between, on the one hand, the method and criteria used and, on the other hand, the result achieved by the automated decision. The information disclosed must enable the data subject to check whether it is true and whether the automated decision in question is indeed based on accurate information.

Recalling its case law (Case C-268/21, judgment of 2 March 2023, *Norra Stockholm Bygg*), the Court of Justice reiterates that a national court may consider that the personal data of the parties or third parties must be communicated to it to be able to consciously balance, in compliance with the principle of proportionality, the interests

[44] U. Mylly, *Transparent AI? Navigating between rules on trade secrets and access to information*, in *IIC-International Review of Intellectual Property and Competition Law* 54, 2023, 1013 ss.

at stake, namely access to its own data used on the one hand and industrial confidentiality on the other. The result of that balancing allows the national court to authorize the full or partial disclosure to the other party of the personal data thus disclosed if it considers that such disclosure does not go beyond what is necessary to ensure the effective enjoyment of the rights that individuals derive from art. 47 of the Charter of Fundamental Rights of the European Union concerning the right to an effective remedy. Such a principle may also apply to the information referred to in art. 15(1)(h) of the GDPR, even when it competes with the rights under art. 2(1)(1) of Directive 943/2016.

The Advocate General concludes that in the case of subjecting a person to an automated decision-making process as understood by art. 22 GDPR, meaningful information on the logic used, including profiling, concerns the method and criteria used by the data controller. They must be concise, easily accessible, understandable, and formulated in simple and clear language. They must also be sufficiently complete and contextualized to enable that person to verify their accuracy and whether there is a coherence and an objectively verifiable causal link between, on the one hand, the method and criteria used and, on the other hand, the result reached by the automated decision in question, so that the latter can be challenged knowingly by the data controller according to art. 15(1)(h) GDPR.

On the contrary, the data controller is not obliged to disclose complex technical information, such as instructions in a programming language, which would not be understood by laypeople who possess no specific expertise. Therefore, the Advocate General considers the disclosure of the algorithm used in the automated profiling process excludable.

4. The right to technical interpretability and AI automated decision-making

In our opinion, the Advocate General's solution is not satisfactory, and additional considerations are necessary.

First, the right to explanation is not stated in GDPR only, but also in Convention 108+, which is the only binding international legal instrument on the protection of personal data[45]. Convention 108+ applies to all personal data processing activities without limitation to sectoral distinctions. It includes data processing in justice, combating crime, defense, public safety, and state security. This is in contrast to the EU's GDPR, which has specific exclusions for activities such as state security and certain criminal justice matters[46]. Unlike older iterations or other frameworks, it no longer allows countries to exempt entire categories of data processing, such as those related to state security,

[45] C. Gallese, *Legal Aspects of AI in the Biomedical Field. The Role of Interpretable Model*s, in B. Carpentieri-P. Lecca (eds) *Big Data Analysis and Artificial Intelligence for Medical Sciences*, Hoboken, 2024, 339 ss.; C. De Terwangne, *Council of Europe convention 108+: A modernised international treaty for the protection of personal data*, in *Computer Law & Security Review* 40, 2021.

[46] However, Convention 108+ is not a self-executing treaty, so implementing legislation is needed, while GDPR does not need implementing laws.

from the Convention's protections. The text does include specific exceptions to ensure that vital public interests like combating crime, state security, or maintaining judicial independence are not hampered. However, these exceptions are narrowly tailored and do not amount to full exemptions for specific data processing categories.

Traditionally, the Convention focused on automated processing of personal data. Convention 108+ now also includes non-automated processing, provided the data is part of a structured, accessible, and retrievable set of information. Examples include paper-based registers, directories, and structured files, which must comply with the Convention's protections if they meet these criteria[47].

In the explanatory note of art. 10 of the Convention, credit scoring is explicitly cited: «Data subjects should be entitled to know the reasoning underlying the processing of their data, including the consequences of such a reasoning, which led to any resulting conclusions, in particular in cases involving the use of algorithms for automated decision-making including profiling. For instance, in the case of credit scoring, they should be entitled to know the logic underpinning the processing of their data and resulting in a "yes" or "no" decision, and not simply information on the decision itself. Without an understanding of these elements there could be no effective exercise of other essential safeguards such as the right to object and the right to complain to a competent authority». This convention is particularly important as it is not only applicable to EU Member States but also to other countries and it is still open to non-signatories members.

Secondly, we advocate for the recognizing of the "right to technical interpretability"[48] as a fundamental right, because, due to technical limitations, employing inherently interpretable models is the only way to protect citizens in high-risks AI applications. Interpretability means employing white boxes (ante-hoc models, glass-box approaches[49]) that are technically transparent, as opposed to black-boxes. In the heated debate on AI explainability, the doctrine, case law, and legislation have not theorized the existence of a right imposing the use of a specific model type from a technical point of view: AI providers and users are free to choose their preferred model.

However, in our opinion, if we consider the systematic interpretation of EU and international legal frameworks surrounding high-risk AI systems, a strong case can be made for establishing interpretability as a legal and ethical standard in this field, and in other sensitive domains as well (e.g., healthcare). High-risk systems that significantly affect individuals' rights and freedoms must be transparent and understandable to ensure accountability. Interpretability allows both the users (e.g., the bank employee) and those affected by these systems (e.g., the consumers) to understand how decisions are made, which is essential for upholding legal standards and protecting fundamental rights, without the need to disclose trade secrets or the algorithm itself.

In contrast, black-box AI systems - those whose internal processes are opaque and not easily understood, even by experts - should be used with caution. These systems

47 C. De Terwangne, *Council of Europe convention 108+,* cit.

48 C. Gallese, *The AI Act proposal: a new right to technical interpretability?* In *arXiv preprint arXiv:2303.17558*, 2023, forthcoming in Milan University Press.

49 A. Holzinger-M. Plass-K. Holzinger-G.C. Crisan-C.M. Pintea-V. Palade, *A glass-box interactive machine learning approach for solving np-hard problems with the human-in-the-loop*, in *Creat. Math. Inform.* 28, 2019, 121 ss.

should only be employed in scenarios where decisions can still be fully evaluated based on factors other than the AI's output, such as on the basis of a human assessment. Relying solely on black-box outputs in critical decisions, especially in high-risk areas like healthcare, law enforcement, or financial services, presents serious risks to fairness, transparency, and accountability.

The definition of "causability"[50] by Holzinger et al. focuses on the essential relationship between AI systems and their users, in particular on how well an explanation supports causal understanding within a given context[51]. This definition assumes the inherent necessity of a causal model that links AI decisions to a framework comprehensible by a human expert to ensure transparency, efficiency, and user satisfaction. On the other hand, Ploug et al.'s perspective diverges by shifting the focus toward contestability[52], focusing on the possibility for patients (or users) to challenge or contest the AI's outputs, which represents a broader view of accountability. Unlike causability, Ploug et al. do not prescribe specific requirements for explainability, which could make their approach more flexible but potentially less grounded in standardized frameworks for interpretability.

These two different approaches are part of a broader debate in AI explainability[53], among which the question is whether the emphasis should lie on precise, causally grounded models tailored to experts or on creating systems open to contestation by different types of stakeholders.

In our opinion, the very possibility of exercising informed consent – the essence of personal autonomy - is compromised when individuals cannot understand how their data is being used or how decisions about them are made. This lack of transparency surely affects informed consent according to GDPR, but it also undermines the ability to challenge decisions that are based on automated decision-making processes (the contestability, as mentioned by Ploug), and even prevents consumers from knowing when they are being systematically discriminated in the first place. In fact, when decisions are generated by a black-box system, it is nearly impossible for an affected individual to appeal or dispute those outcomes, as they have no insight into how or why the decision was made.

Moreover, the absence of interpretability in AI systems directly threatens the exercise of several fundamental rights. For instance, the right to a fair trial can be compromised if consumers have not enough information to file for a case or to defend themselves; the right to self-determination is eroded when decisions impacting employment, credit, or healthcare are made by systems whose logic is inaccessible to the individual; and the right to non-discrimination is also at significant risk, as AI systems can inadvert-

[50] Defined as «as the extent to which an explanation of a statement to a human expert achieves a specified level of causal understanding with effectiveness, efficiency and satisfaction in a specified context of use».

[51] A. Holzinger-G. Langs-H. Denk-K. Zatloukal-H. Müller, *Causability and explainability of artificial intelligence in medicine*, in *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 9(4), 2019.

[52] T. Ploug-S. Holm, *The four dimensions of contestable AI diagnostics-A patient-centric approach to explainable AI* in *Artificial Intelligence in Medicine*, 107, 2020.

[53] The whole debate on AI explainability and interpretability is too extensive to be summarized in the present work.

ently perpetuate biases embedded in their training data[54]. Without transparency, it is difficult to detect or rectify discriminatory practices, a circumstance that undermines equality and fairness.

Given these concerns, it is clear that black-box systems should only be permissible in situations where their sole outputs do not determine the outcome of a decision. In such cases, there must be strong safeguards in place, including meaningful human oversight[55] and the consideration of other non-AI-based factors. This ensures that decisions remain accountable and can be scrutinized for fairness, accuracy, and compliance with human rights standards.

Ultimately, the lack of technical interpretability in AI systems presents significant barriers to justice, equality, and transparency. Since high-risk AI systems become increasingly integrated into daily decision-making processes that impact fundamental rights, interpretability must become the standard. This will ensure that automated systems remain accountable and that individuals retain the ability to challenge and understand the decisions that affect them. For this reason, we believe that there is room in the current EU legal system to theorize the existence of a right to technical interpretability.

Having explored the implications of art. 22 GDPR, it's time to turn our attention to art. 86 AI Act.

5. Is a remedial coexistence between art. 22 GDPR and art. 86 AI Act possible?

Art. 86 AI Act[56] plays a similar role to art. 22 GDPR and recognises the right to an individual explanation for the benefit of any person who has been affected by a decision made by the deployer based on the results of a high-risk AI system. The article provides that citizens who were affected by legal or similar significant effects in a way which that they consider to have a negative impact on their health, safety or fundamental rights, have the right to obtain - from the person in charge of the deployment -

[54] C. Gallese et al., *Investigating Semi-Automatic Assessment of Data Sets Fairness by Means of Fuzzy Logic,* in *2023 IEEE Conference on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB)*. IEEE, 2023.

[55] Keeping in mind that «The controller cannot avoid the Article 22 provisions by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing», Working Party 29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2017.

[56] The text of art. 86 reads: «1.Any affected person subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system listed in Annex III, with the exception of systems listed under point 2 thereof, and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights shall have the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken. 2.Paragraph 1 shall not apply to the use of AI systems for which exceptions from, or restrictions to, the obligation under that paragraph follow from Union or national law in compliance with Union law. 3.This Article shall apply only to the extent that the right referred to in paragraph 1 is not otherwise provided for under Union law.».

clear and meaningful explanations on the role of the AI system in the decision-making process and on the main elements of the decision taken.

The article provides for an exception in the case of AI systems employed in critical infrastructures, that is those intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity. Such systems are essential to public safety and economic stability and ensure the very survival of the population. Disclosing sensitive information about how AI systems operate within these critical infrastructures could inadvertently expose vulnerabilities, making them targets for cyberattacks or sabotage that could represent a risk for life. For example, detailed explanations of AI decision-making processes in these systems could reveal weaknesses in algorithms or operational dependencies, which malicious actors could exploit to disrupt essential services. In addition, if the deployers of high-risk AI systems were required to provide detailed, case-by-case explanations for decisions, it could create operational delays, legal disputes, or administrative burdens that might affect the efficient functioning of these systems.

Legislators have applied the principle of proportionality in crafting this exception, as the harm caused by requiring individualized explanations could outweigh the benefits of having an explanation. In these contexts, a clear explanation at the individual level might not be as feasible or as necessary as it would be for other high-risk AI systems impacting health, employment, or finances. Therefore, legislators recognized that the public interest in maintaining the safety and reliability of critical infrastructure outweighs the individual's right to a detailed explanation in these specific contexts.

The text of art. 86 of Regulation EU 1689/2024 appears innovative, but the protections granted by this provision remain insufficient[57]. Our critique of art. 86 of Regulation EU 1689/2024 is caused by a fundamental issue in the allocation of responsibility for providing explanations to individuals affected by decisions made using high-risk AI systems. While the article is a decisive step in granting individuals the right to obtain "clear and meaningful" explanations of the role of AI in decision-making as opposed to the mild art. 22 GDPR, we argue that the protections it offers remain unsatisfactory due to a significant gap in accountability.

Under the article, the responsibility for responding to individuals' requests for explanations is placed solely on the deployer of the AI system, that is the entity that implements and uses the system in practice. This means that the deployer is tasked with addressing concerns from affected individuals and providing the required explanations. However, this approach excludes the provider of the AI system, the entity that develops, designs, or supplies the underlying algorithm and methodology on which the system operates. The exclusion of the provider from the duty to reply is problematic because a third-party deployer may not possess sufficient technical knowledge to fully explain how the AI system operates at a deeper, systemic level. Deployers, for instance, might only understand how the AI system is applied in a specific context, such as making hiring decisions, loan approvals, or resource allocations, but they may lack insight

[57] S. Wachter, *Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond*, in *Yale Journal of Law and Technology*, 26, 2024, 693.

into the design choices, data collection practices, and training methods that constitute the core of the AI's decision-making process. Since the provider is the one responsible for creating the system and determining how data is collected and processed, excluding them from the obligation to provide explanations leaves a significant gap in transparency and accountability every time deployers and providers are different entities.

This gap can result in explanations that are incomplete or superficial, depriving individuals of meaningful insight into how decisions affecting their lives are made. For example, if an individual challenges an AI-based mortgage decision, the deployer may be able to explain how the system was applied in practice but may not be able to address deeper questions about potential biases in the algorithm or the fairness of its training data. Without access to this technical information from the provider, the individual's ability to challenge the decision or seek justice is significantly undermined.

We argue that responsibility for responding to individuals' concerns should be shared between the deployer and the provider. The deployer should explain the practical aspects of how the AI system was used in the specific context of the decision, while the provider should be required to disclose technical details about the algorithm's design, its data processing methodology, and safeguards to ensure fairness and compliance. This shared responsibility would ensure that individuals receive meaningful explanations, addressing both the practical and technical dimensions of the decision-making process.

Since art. 86 places the entire burden of explanation on the deployer, it risks creating an accountability gap that undermines the regulation's goals of transparency and fairness. Deployers may struggle to provide full explanations, while providers, who are often in the best position to explain the system's functioning, are not required to engage with individuals at all. This circumstance limits the protections granted to individuals, making it harder for them to understand and challenge decisions that negatively affect their rights, health, or safety.

Additionally, the boundary for application of art. 86 is strict. This article is applicable only to high-risk AI systems, and it is only triggered if the AI decision has a significantly adverse impact on the health, safety, or fundamental rights of the user[58]. This means that harmful non-high-risk systems are excluded by this provision, despite their impact might be equally significant. For example, with the widespread use of generative AI systems – some of which even posing systemic risks – more and more individuals are forced to interact with chatbots and other automatic systems that perform a preliminary screening their requests (e.g., client service, online credit applications), finding themselves without protection despite being significantly affected by the general purpose AI system's decision.

Regarding what fundamental rights fall within the scope of credit scoring, it is argued that processing data concerning a person's reputation and dignity makes this tool available to the subject of credit profiling. Incorrect reporting as a bad payer could have significant consequences on the reputation of the person being ranked, which should be solid and adherent to reality. The damaging effects of an erroneous ranking or one

[58] H. van Kolfschooten-J. van Oirschot, *The EU Artificial Intelligence Act: Implications for healthcare*, in *Health Policy*, 149, 2024.

based on fallacious data or for derisory figures could cause damages, even if the resulting misfortunes are not comparable to those of Jean Valjean, who found himself a convict for a piece of bread stolen out of hunger.

According to GDPR, data subjects have the right to request a review or reconsideration of the automated decision, and they can ask for human intervention; in the case of an explanation request, if the answer obtained by the operator is not satisfactory, to whom can the subject person requesting the explanation turn? In the writers' opinion, there are three possibilities of appeal:

1. if, in the criticised automated decision, the requesting party finds a case of inadequate data processing within the meaning of the GDPR, the requesting party may appeal to the national supervisory authorities (art. 77 GDPR);
2. if the supervisory authority fails to address a complaint or respond in a timely manner, individuals can lodge a complaint against said authority to the courts of the Member State where the supervisory authority is based (art. 78 GDPR);
3. the ordinary courts are on the ground that the unlawful processing of personal data violates fundamental rights[59] (arts. 79 and 82 GDPR).

For issues that involve cross-border processing or interpretation of EU law, appeals can also be escalated to the CJEU.

One may wonder whether art. 86 competes with the remedy under art. 22 GDPR since the latter expressly refers to decision-making processing in the sense that it produces and enforces a decision having direct or indirect effects on the data subject. Nonetheless, the answer would seem to be negative, since it is only art. 86 that explicitly recognises that the explanation must be clear and meaningful, whereas the current text of art. 22 GDPR establishes «at least the right to obtain human intervention by the controller, to express one's opinion and to contest the decision» by the person subject to the automated decision[60]. Apparently, therefore, two distinct rights could be considered to be coexisting: art. 22 GDPR recognising the right to human intervention in data processing and art. 86 absorbing the right to request clear and meaningful explanations of the decision-making process for those parts of the latter that are not linearly explicable.

In addition, another difference is that art. 22 GDPR only refers to decisions taken on personal data only, while anonymized data are excluded. On the contrary, art. 86 AI Act has a broader scope, since it refers to any high-risk system, regardless of the data employed for its training, testing, validating, or those in the input and output. Therefore, even decisions made based on aggregated data or historical data, that affect a person or a group of persons despite not employing their personal data, must be explained. For example, if a bank decides to deny credit not to a specific customer but to an entire group of customers, based on the determinations of an algorithm that

[59] For example, under the Italian criminal code, the unlawful personal data processing might constitute a criminal offense.

[60] For an analysis of art. 22 GDPR and AI, see the works of Prof. Pagallo. U. Pagallo, *Algoritmi e conoscibilità*, in *Rivista di filosofia del diritto*, 2020, 9.1: 93 ss.; U. Pagallo, *Algo-rhythms and the beat of the legal drum*, in *Philosophy & Technology*, 2018, 31.4: 507-524. See also M. Palmirani et al., *Interpretabilità, conoscibilità, spiegabilità dei processi decisionali automatizzati*, in: *XXVI lezioni di Diritto dell'Intelligenza Artificiale*, Torino, 2021, 66 ss.

examined national statistics, an explanation must be provided to affected individuals. Art. 86 also closely correlates with other GDPR provisions. Arts. 13(2)(f) and 14(2)(g) GDPR explicitly address automated decision-making, including profiling, when it produces legal or similarly significant effects on individuals. These provisions require data controllers to inform individuals about a) the existence of automated decision-making, b) the logic involved in these decisions, c) the significance and potential consequences of such processing for the individual. Thus, both frameworks target automated processes that impact individuals in legally or materially significant ways, but while the GDPR limits its focus to the use of personal data, the AI Act applies more broadly to high-risk AI systems, whether or not personal data is involved.

6. The comparative case-law following the *SCHUFA* ruling

In Austria, the subject of the assessment of the Bundesverwaltungsgericht (BVwG) is whether the automated creditworthiness determination procedure and whether such a decision falls under the discipline of art. 22 GDPR concerning access to the explanation of the automated decision. Applying the principles elucidated by the judgment of the Court of Justice of the European Union *SCHUFA* (C-634/21 OQ/Land Hessen), the Federal Administrative Court ruled that the automated calculation of a probability value by a credit information agency, based on personal data, is an «automated individual decision» when a third party relies on that value to establish, implement or terminate a contract with the person concerned.

In the present case, the BVwG held that the probability value provided by the holder to the energy supplier was decisive for the refusal to conclude a contract with the data subject, thus constituting an automated decision with significant legal effects within the meaning of art. 22 of the GDPR.

The BVwG also rejected the data controller's argument that the credit score was only a preparatory calculation, as this interpretation could circumvent art. 22 of the GDPR. In addition, the federal administrative courts ruled that none of the exceptions in art. 22(2) GDPR applied to the case, rendering the automated processing unlawful. The data controller also violated the principles of "lawfulness" and "fairness" under art. 5(1)(a) of the GDPR.

In Germany, the Landgericht Traunstein (LG Traunstein) ruled that art. 22(1) of the GDPR only applies when an automated decision has «legal effects» on the data subject, such as in the case of a contract rejection. Citing the EU Court of Justice, he clarified that an agency credit score only falls under art. 22 if it is the only criterion used in the decision-making process.

The court also clarified that data controllers do not bear the burden of proof for all GDPR requirements but only for the lawfulness of the processing. Therefore, the subject had to prove that the holder had violated art. 22(1) but failed to provide sufficient evidence. The legal process, in its fairness, also allowed the holder to prove that the subject had recently concluded contracts, disproving the idea of discrimination based

on credit score. The Landgericht also rejected the allegation of discrimination, stating that age, gender, or address were not considered in the calculation of credit scores. As there was no evidence of a breach of the GDPR or harm suffered, the art. 82's claim was dismissed. The court concluded that the data subject's request for access to the data was satisfied and that the data controller could protect its trade secrets under art. 15(4) of the GDPR. On those grounds, the case was finally dismissed.

Those rulings are important as they clarify the boundaries of GDPR, however, they do not adequately consider systemic issues of discrimination. For example, as shown by multiple computer science works[61], even when "age, gender, or address" are not directly employed in a machine learning system, the algorithm can infer those characteristics by analysing strictly correlated dataset attributes. As recognized by legal scholarship[62], despite inferences can be as harmful as the personal data they refer to, in the era of big data and social media there is still a need to protect citizens from harmful inferences.

In the United States[63], on the one hand, there was—and it remains relevant today—a deep controversy regarding the presence of bias. Access to credit became an issue linked to the Civil Rights Movement[64], as racial elements were considered in credit profiling.

From a regulatory point of view, the Fair Credit Reporting Act of 1970, and later the amendments contained in the Equal Credit Opportunity Act of 1974, were enacted to ban the use of race, sex, and other personal traits in lending.

On the other hand, these laws prohibited financial and credit institutions from using information that could profile applicants in a discriminatory way. However, lenders were still able to use information indirectly related to these prohibited characteristics, such as postcodes, which revealed the social and racial background of applicants, including their ethnic origins[65]. This circumstance effectively preserved the influence of race in lending decisions[66].

As a result, a paradoxical effect has emerged: the use of statistical models and black-box algorithms[67] has not eliminated racial discrimination but has instead made it more challenging to identify.

---

[61] A. Fabris, *Measuring fairness under unawareness of sensitive attributes: A quantification-based approach*, in *Journal of Artificial Intelligence Research*, 76, 2023, 1117 ss.

[62] S. Wachter-B. Mittelstadt, *A right to reasonable inferences: re-thinking data protection law in the age of big data and AI*, in *Columbia Business Law Review,* 2019, 494; D. Clifford-M. Richardson–N. Witzleb, *Artificial intelligence and sensitive inferences: new challenges for data protection laws* in M. Findlay–J. Ford-J. Seah–D. Thampapillai (eds), *Regulatory Insights on Artificial Intelligence,* Cheltenham, 2022, 19 ss.

[63] B. Kiviat, *Credit scoring in the United States,* in *economic sociology_the european electronic newsletter,* 21(1), 2019, 33-42; J. Lauer, *Creditworthy: A History of Consumer Surveillance and Financial Identity in America,* New York, 2017, *passim.*

[64] B. Kiviat, *Credit scoring*, cit.; J. Laurer, *Creditworthy,* cit.; G. R. Krippner, *Democracy of Credit: Ownership and the Politics of Credit Access in Late Twentieth-Century America*, in *American Journal of Sociology*, 123, 2017, 1 ss.

[65] L. Hyman, *Debtor Nation: The History of America in Red Ink,* Princeton, 2011, *passim.*

[66] E. Cohen-Cole, *Credit Card Redlining*, in *The Review of Economics and Statistics* 93, 2011, 700 ss.

[67] F. Pasquale, *The black box society: The secret algorithms that control money and information,* Cambridge, 2011, *passim.*

Some recent studies[68] have investigated the impact of algorithms on the approval of monthly mortgage applications and have found that the gap between white and black applicants in the approval of applications is decreasing[69]. One may wonder whether this result is due to lawsuits filed over issues of discrimination in access to credit[70]. These cases highlighted the "reverse redlining" effect of creating and utilizing minorities and identifying a trusted social network to induce them to take out mortgages with high rates. Indeed, such disputes were connected to the financial crisis triggered by subprime mortgages, which began in the late 1980s and 1990s and exploded in the 2000s. This crisis was preceded by a shift in the evaluation of credit scoring, which no longer focused on the borrower's actual ability to repay the loan but rather on the security of repayment by reliable customers. This assessment was separate from the evaluation of the risk associated with less reliable customers, who were not denied loans but were instead subjected to higher costs. Indeed, this different credit scoring evaluation «brings more people into the market and expands the definition of who is "creditworthy," but at the same time, it demarcates new moral boundaries, such as those between "prime" and "subprime" borrowers»"[71].

Also in the United States, credit scoring has been the subject of judicial litigation that has reached the highest levels of jurisdiction. The US Supreme Court[72], a key player in shaping the legal landscape, unanimously ruled that the Fair Credit Reporting Act (FCRA) does not grant absolute immunity to the federal government (and federal agencies) in the case of erroneous debt reporting that impairs credit scores, thus allowing the federal government to be held liable for reporting. Justice Neil Gorsuch said the FCRA allows consumers to sue anyone who intentionally or negligently provides false information, including government agencies. The law defines "person" as any individual, company, government, or agency, indicating that the federal government can be liable.

According to the US Supreme Court, the issue is resolved by deferring to the principle of representative democracy because the will of the people, expressed by Congress[73], was to provide a remedy when the federal government violates a person's right to accuracy in credit reporting.

---

[68] A. C. B. Garcia-M. G. P. Garcia, R. Rigobon, *Algorithmic discrimination in the credit domain: what do we know about it?,* in *AI & SOCIETY*, 39(4), 2024, 2059 ss., spec. 2079; E. Yu, *Banking trends discrimination in mortgage markets*, in *Banking Trends* 7, 2022, 2 ss.; M. Giacoletti-R. Heimer-E. G. Yu, *Using high-frequency evaluations to estimate discrimination: Evidence from mortgage loan officers,* in *Proceedings of Paris December 2021 Finance* Meeting *EUROFIDAI-ESSEC,* 2021.

[69] E. Yu, *Banking trends discrimination in mortgage markets*, cit., 4.

[70] These cases are: *Baltimore vs. Wells Fargo Bank; City of Memphis vs. Wells Fargo Bank; Adkins et al. v. Morgan Stanley, Barkley v. Olympia Mortgage.* All these cases addressed predatory loans in violation of the Fair Housing Act. L. B. Hearit, *JPMorgan Chase, Bank of America, Wells Fargo, and the financial crisis of 2008,* in *International Journal of Business Communication*, 55, 2018, 237 ss.

[71] B. Kiviat, C*redit scoring in the United States,* cit. 36.

[72] 601 U.S. 42 (2024).

[73] E. B. Wydra-B. J. Gorod-M. Becker-Cohen, *United States Department of Agriculture Rural Development Rural Housing Service v. Kirtz*, 2024.

7. Conclusions

The *SCHUFA* decision by the CJEU represents an important precedent in the case law interpretation art. 22 of the GDPR, and it highlights that transparency and accountability in automated decision-making processes is still an issue for large companies. The innovative aspect of this ruling is that it recognizes credit scores as decisions with legal effects, even when they serve as intermediary steps in a larger decision-making chain.
Subsequent case law shows the far-reaching implications of the SCHUFA precedent. The Austrian and German court decisions refine the application of art. 22 GDPR, giving nuanced interpretations of what constitutes an automated decision and the extent of data controllers' obligations. However, these rulings collectively point towards growing judicial recognition of the need to balance individual rights with the legitimate interests of businesses in protecting their proprietary algorithms, without adequately considering issues of systemic discrimination posed by harmful inferences.
The introduction of art. 86 in the AI Act represents a complementary approach to addressing the challenges posed by high-risk AI systems. While it shares similarities with art. 22 GDPR, its broader scope and explicit focus on clear and meaningful explanations potentially offer enhanced protection for individuals affected by AI-driven decisions. However, the limitations in its applicability to only high-risk systems and the ambiguity surrounding the definition of "significantly adverse impact" may restrict its effectiveness in certain scenarios.
The comparative analysis, including the U.S. Supreme Court's ruling on the Fair Credit Reporting Act, shows that the challenges associated with credit scoring and automated decision-making are global. The decision to allow liability for erroneous reporting, even for government agencies, reflects a growing international consensus on the importance of the accountability principle in credit reporting systems.
The legal framework on credit scoring and AI-driven decision-making systems will likely continue to develop within the Digital Strategy[74]. The tension between the right to explanation, protection of trade secrets, and the need for algorithmic transparency remains an important area for future legal and policy development. The concept of a "right to technical interpretability" can be seen as a possible solution to protect citizens' rights without compromising intellectual property, as inherently interpretable models in high-risk applications are able to give clear explanations of the logic involved in the decision-making process. In light of the jurisprudence on credit scoring and automated decision-making, recognizing the existence of a "right to technical interpretability" becomes even more important. This right, while not explicitly codified in current legislation, can be inferred from the spirit of existing regulations such as the

[74] The Digital Strategy represents the European Union's focus on data, such as on the protection of personal data and the harmonization of data sharing practices, has been a priority since the Maastricht Treaty (1993), which significantly deepened EU integration. After the Maastricht Treaty, the EU began to enact the regulation of data to balance the need for privacy with the free flow of information necessary for economic and social integration. As early as the 1995, the Database directive was enacted, followed by the Data Protection Directive the same year. For an examination of the Digital Strategy, see C. Gallese, *A first commentary to the proposal for a new Regulation on fair access and use of data (Data Act)*, in *Media Laws*, 3, 2022, 237 ss.

GDPR and the AI Act, as well as from the judicial interpretations provided by courts across jurisdictions.

The SCHUFA implicitly acknowledged the need for interpretability in those systems. Other case law, including the Austrian and German court decisions, further refines this concept and highlights the importance of clear explanations of automated decisions when they have legal or similarly significant effects on individuals. This trend in judicial reasoning supports the idea that technical interpretability should be a fundamental right, especially in high-risk AI applications like credit scoring, as black-box models are so opaque that it is barely impossible to reach true transparency[75].

The introduction of art. 86 in the AI Act represents a step towards codifying aspects of the right to technical interpretability. Since it codifies the requirement of providing "clear and meaningful explanations" for decisions made by high-risk AI systems, it acknowledges the necessity of making complex technical processes comprehensible to those affected by them, complementing and expanding the transparency principle that is found in many Digital Strategy provisions. However, the limitations in its applicability greatly undermine its legal impact, as harmful non-high-risk systems, such as those based on Generative AI[76], are excluded by this provision.

The ongoing doctrinal, judicial, and legislative developments in this field need to move forward with a different approach that safeguards citizens' rights instead of siding with corporate interests. As AI systems become increasingly integrated into decision-making processes, impacting fundamental rights, the legal framework must at least ensure that all companies employing automated systems - not only those producing high-risk systems - remain accountable to those affected by their decisions. Although trade secrets should be preserved, this cannot happen at the expense of consumers. It is important that case law is able to keep up with the latest technological developments (such as Generative AI) and understand their impact on citizens and the whole society.

[75] C. Gallese, *The AI Act proposal: a new right to technical interpretability?,* cit.

[76] C. Gallese, *Web scraping and Generative Models training in the Directive 790/19*, in *i-lex* 16.2 2023, 1 ss.

Brevi riflessioni sulla disciplina della par condicio: tra la "necessarietà costituzionale" dei principi ispiratori e l'urgenza di un aggiornamento*

Giorgio Sichera

Abstract

L'articolo propone un'analisi dei profili costituzionalistici della legge sulla *par condicio*, domandandosi se, in un tempo segnato da profondi mutamenti nei modi e nei tempi dell'informazione e della comunicazione politica, una disciplina di tal genere risponda ancora o meno a un "imperativo costituzionale". La riflessione prende in esame il comunicato AGCOM del 15 maggio 2024, e le conseguenze dello stesso sulla (mancata) organizzazione di confronti televisivi tra gli esponenti politici coinvolti nelle elezioni europee. Mettendo così in luce sia gli aspetti anacronistici (come l'applicazione del solo criterio matematico del conteggio delle presenze) che al contempo quelli costituzionalmente necessari della disciplina (che è un mezzo di limitazione del potere proprio del costituzionalismo democratico), si propongono in conclusione delle riflessioni sul futuro della *par condicio* e sull'ineludibile legame della stessa con il sistema elettorale di riferimento.

The article offers an analysis of the constitutional profiles of the *par condicio* law, questioning whether, in an era marked by profound changes in the methods and timing of information and political communication, such regulation still responds to a "constitutional imperative". The discussion examines the AGCOM statement of May 15, 2024, and its consequences on the (lack of) organization of televised debates among political representatives involved in the European elections. By thus highlighting both the anachronistic aspects—such as the application of the mere mathematical criterion of attendance counting—and, at the same time, the constitutionally necessary elements of the regulation—as a means of limiting power inherent in democratic constitutionalism—the article ultimately offers reflections on the future of *par condicio* and its inextricable link with the relevant electoral system.

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

Giorgio Sichera

Sommario

Keywords

Par condicio – pluralismo informativo – comunicazione politica – piattaforme digitali – sistemi elettorali

1. Introduzione: una disciplina necessaria ma inattuale?

L'art. 48 della Costituzione prevede esplicitamente che il voto sia "libero", ovvero che consista nell'espressione dei convincimenti e della coscienza di ciascun elettore. Con ciò non si intende soltanto che l'elettore debba essere "protetto" da coazioni o minacce di violenza fisica, ma altresì che egli non debba essere sottoposto a indebite forme di pressione o a influenze psicologiche, in grado di pregiudicare la libertà e la spontaneità della manifestazione della propria volontà elettorale[1].

Da tale principio si ricavano due ordini di divieti: alcuni direttamente sanzionabili, in quanto consistenti in violenze o minacce, fisiche o psicologiche, esercitate direttamente da terzi a danno degli elettori[2], altri derivanti dalla cd. "legislazione elettorale di contorno", che disciplina le campagne elettorali e pone limiti allo svolgimento dell'azione di comunicazione e propaganda politica. Da ciò discende che per tutelare la libertà del voto non è sufficiente – seppur certamente necessario – prevedere sanzioni a carico di terzi che influenzano in maniera diretta, per l'appunto con violenze o minacce fisiche o psicologiche, la volontà dell'elettore, bensì è necessaria la presenza di una regolamentazione che garantisca che il momento di formazione del voto si svolga in condizioni di parità di opportunità tra i concorrenti, a prescindere dalle risorse (prima di tutto economiche) di cui dispongono i partiti politici che partecipano alle elezioni. Il rispetto dell'uguaglianza di opportunità tra i candidati tutela infatti «l'uguaglianza formale della cittadinanza rispetto alla concentrazione sostanziale dei poteri di fatto»[3]. Ciò detto, la disciplina che regola la cd. "*par condicio*" costituisce un esempio di legislazione costituzionalmente necessaria, volta cioè a tutelare un interesse costituzionalmente rilevante – la libertà del voto, ma anche la personalità, la segretezza e

[1] E. Grosso, *Art. 48*, in R. Bifulco-A. Celotto-M. Olivetti (a cura di), *Commentario alla Costituzione*, vol. I, Torino, 2006, 971.

[2] Artt. 96, 97 e 100 d.P.R. 361/1957, con le aggravanti di cui all'art. 101 per l'utilizzo di violenze, minacce, pressioni, disordini, mediante armi, o si sia agito anonimamente o a nome di «gruppi di persone, associazioni o comitati esistenti o supposti».

[3] F. Lanchester, *La propaganda elettorale (e referendaria) in Italia tra continuità sregolata e difficile rinnovamento*, in *Quaderni Costituzionali*, 3, 1996, 386.

l'uguaglianza – che rimarrebbe altrimenti sprovvisto di tutela. Si tratta pertanto di un testo normativo che garantisce l'effettività delle garanzie costituzionali relative al diritto di voto, ovvero che ciascun elettore sia concretamente posto nelle condizioni di esprimere la propria scelta elettorale in maniera libera e consapevole[4].

Richiamando in termini generali e introduttivi un dibattito assai complesso e risalente nella dottrina costituzionalistica[5], le critiche sulla *par condicio* si fondano sull'assunto che una legislazione in termini di libertà di informazione politica sia propria di uno Stato paternalista, preoccupato dal fatto che le opinioni dei cittadini possano essere manipolate. Il rischio è quello che i pubblici poteri finiscano per "prescrivere" una "dieta informativa" ai cittadini, non scommettendo di fatto sulla capacità degli stessi di formarsi una propria opinione.

Tali critiche sono contrassegnate da innegabili elementi di ragionevolezza, essendo la libertà di manifestazione del pensiero quella che più delle altre contribuisce a definire una forma di Stato[6], e dunque, specie in ambito politico, la libertà che per eccellenza i pubblici poteri devono il più possibile astenersi dal limitare. Si ritiene tuttavia che quella sulla *par condicio* non sia una legislazione volta a tutelare primariamente (di certo non esclusivamente) il bene costituzionalmente protetto della corretta formazione

[4] E. Grosso, *Art. 48*, cit., 972.
Con riferimento alle consultazioni referendarie, tale principio, riguarda non solo la parità di opportunità per i comitati nel corso della campagna, ma anche la "chiarezza" del quesito, che deve altresì essere riconducibile a un'unità concettuale (omogeneità) e privo di contraddizioni. (Corte cost., 7 febbraio 1978, n. 16; G. Zagrebelsky - V. Marcenò - F. Pallante, *Lineamenti di diritto costituzionale*, Milano, 2019, 450). La finalità è la medesima: il comitato promotore, nel formulare il quesito referendario, non può trarre in inganno né influenzare il libero convincimento del corpo elettorale. Vi è inoltre da chiedersi se l'invito all'astensionismo trovi tutela costituzionale, e possa dunque rispettare il dettato dell'art. 48 Cost. che definisce il voto un «dovere civico» (erano previste delle "sanzioni", "cancellate" nel 1993). Ci si trova in un caso particolare: il voto è una libertà positiva, a cui, di regola, dovrebbe fare da contraltare una libertà negativa; la Costituzione sembra fare un'eccezione, prevedendo il voto come dovere civico, il cui esercizio è pertanto "raccomandato", seppur non normativamente imposto. Si è in altre parole di fronte a un dovere non sanzionabile direttamente a livello giurisdizionale, che però le istituzioni democratiche e la società civile latamente intesa sono tenute a far rispettare. Da ciò parrebbe potersi sostenere – è la posizione della dottrina che non riconosce solo valore esortativo, ma anche normativo all'art. 48 c. 2 (C. Mortati, *Istituzioni di diritto pubblico*, Padova, 1976, 435; E. Bettinelli, *Diritto di voto*, in *Digesto delle Discipline Pubblicistiche*, vol. 5, Torino, 1990, 231, M. Iacometti, *Sull'obbligatorietà del voto nelle consultazioni popolari dell'ordinamento giuridico italiano*, in *Rivista trimestrale di diritto pubblico*, 1, 1982, 56; G. Cordini, *Il voto obbligatorio*, Roma, 1988, 92 ss., per cui un'eventuale reintroduzione di sanzioni all'astensionismo potrebbe essere costituzionalmente legittima, non essendosi la Costituzione limitata a qualificare il voto soltanto come diritto – che non vada riconosciuta tutela all'invito all'astensionismo (seppur difficilmente sanzionabile nella forma di Stato democratico). Con riferimento alle consultazioni referendarie *ex* art. 75 Cost., l'astensionismo ha invece un'influenza sul risultato elettorale (ha cioè un «preciso effetto giuridico» (E. Grosso, *Art. 48*, cit., 973), essendo previsto un *quorum* di validità dall'art. 75 Cost., per cui non sarebbe sanzionabile la propaganda a favore dell'astensionismo (la dottrina su questo è unitaria), ovvero il legislatore non potrebbe discrezionalmente prevedere una sanzione. Tuttavia, il valore esortativo dell'art. 48 c. 2 resta: le democrazie devono avere gli strumenti per "sostenere" le disposizioni costituzionali. Con riferimento alle consultazioni referendarie, cfr. anche AGCOM, delibera 89/14/CONS, "Disposizioni di attuazione della disciplina in materia di comunicazione politica e di parità di accesso ai mezzi di informazione relative alle campagne per i referendum consultivi, propositivi e abrogativi indetti in ambito locale su materie di esclusiva pertinenza locale".

[5] Cfr. F. Modugno, *Par condicio e Costituzione*, Milano, 1997, 348 ss.; E. Bettinelli, *Par condicio. Regole, opinioni, fatti*, Torino, 1997.

[6] R. Zaccaria-A. Valastro-E. Albanesi, *Diritto dell'informazione e della comunicazione*, Padova, 2013, 2; L. Paladin, *Libertà di pensiero e libertà di informazione: le problematiche attuali*, in *Quaderni Costituzionali*, 1,1987, 5.

dell'opinione dei soggetti destinatari della comunicazione politica (soggetti che i poteri pubblici dovrebbero, secondo la logica precedentemente descritta, "difendere"), bensì sia un tipico strumento (costituzionalmente necessario) di limitazione del potere: mirando a parificare le possibilità nell'accesso ai mezzi di comunicazione politica si garantisce l'uguaglianza e la libertà nel confronto tra le opinioni, e dunque la democraticità effettiva della competizione elettorale. All'interno di questa cornice verrà, di conseguenza, garantita la possibilità del cittadino di formarsi una propria opinione, di confermare o modificare i propri convincimenti, scegliendo da sé quale "dieta mediatica" seguire. Se non vi è *par condicio*, tale possibilità (che è una conseguenza della limitazione della concentrazione dei poteri di fatto) gli viene negata, o viene quanto meno indebolita, e – appunto – lo si induce a restare più facilmente "ingabbiato" nel proprio modo di pensare[7].

Sebbene il mezzo televisivo rimanga ancora quello maggiormente utilizzato dai cittadini italiani per informarsi[8], non può farsi a meno di considerare che il tema della *par condicio* interessa anche i nuovi mezzi di comunicazione, su tutti i cd. "*social media*", il cui utilizzo è sempre più diffuso, e che presentano delle difficoltà specifiche riguardo alle tipologie di intervento (si tratta di piattaforme esclusivamente gestite da soggetti privati privi di una responsabilità editoriale[9], in cui circolano notizie essenzialmente

[7] Il modo in cui funzionano le cd. "*filter bubbles*" spiega bene questo meccanismo; si rinvia a riguardo, per tutti, a E. Parisier, *The filter bubble: what the internet is hiding from you*, New York, 2011 e a D. Palano, *Bubble Democracy. La fine del pubblico e la nuova polarizzazione*, Brescia, 2020.
Strettamente connesso, seppur distinto, è il tema – cui solo si fa rinvio – della sanzionabilità di comportamenti che violano la legislazione elettorale di contorno. Fino a che punto in un contesto democratico è possibile prevedere delle sanzioni in seguito a comprovate irregolarità in tema di rispetto della libertà di voto ex art. 48, ovvero della disciplina della *par condicio* in tema di informazione e comunicazione elettorale? È eventualmente possibile intervenire anche a "risultato elettorale acquisito"? Va' fatto notare a riguardo che è estremamente complicato trovare un nesso di causalità determinate tra il mancato rispetto della disciplina e il risultato elettorale in sé; l'esito delle elezioni dipende da molteplici fattori, per cui è difficile stabilire se un comportamento realizzato in violazione di una norma, o la proliferazione di notizie false (si pensi ad esempio al caso della Brexit, in cui è stato provato che il fronte del "*leave*", poi risultato vincitore nella consultazione referendaria, ha basato la propria campagna su inequivocabili *fake news*, per cui si rinvia a J. Cassidy, *How post-truth politics transformed and shaped the outcome of the 2016 Brexit referendum*, in S. Giusti-E. Piras (a cura di), *Democracy and fake news*, Londra, 2021, 53 ss.), sia stata influente o addirittura decisiva nello stabilire l'esito elettorale. Si rinvia in tal senso alle recenti vicende sia in ambito nazionale (relativamente alle elezioni regionali tenutesi nel 2024 nella Regione Sardegna, in riferimento alle quali il Collegio Regionale di Garanzia elettorale, istituito presso la Corte d'Appello di Cagliari, ha contestato alla Presidente della Regione una serie di violazioni delle norme che regolano il rendiconto delle spese in campagna elettorale) che europeo (la Corte costituzionale della Romania, con sentenza del 6 dicembre 2024, n. 32, ha annullato le elezioni presidenziali per violazioni della legislazione elettorale in tema di rendicontazione delle spese sostenute nel corso della campagna elettorale, nonché per interferenze di Stati esteri; cfr. F. Lanchester, *Comunicato "Le elezioni per il Presidente della Repubblica in Romania e l'intervento della Corte costituzionale",* in *Nomos*, 3, 2024, 1), che paiono aprire alla possibilità di un intervento *ex post* che annulli l'esito elettorale qualora sia stata violata la disciplina elettorale di contorno.
Un altro interrogativo che intercetta il tema della comunicazione politica è quello della propaganda volta più che a informare l'elettore a «deprimere la [sua] attenzione e la stessa capacità di ragionamento» (E. Bettinelli, *Diritto di voto*, cit., 228), ritenuta limitabile da una parte della dottrina proprio in ragione del danno causato a un bene costituzionalmente protetto, su cui restano dubbi circa l'applicabilità al contesto odierno e l'individuazione dell'autorità volta a realizzare un tale intervento.

[8] V. dati citati *infra*, nota 67, par. 3.1.2.

[9] Si rinvia a *infra*, nota 79, par. 4.1.

"disintermediate"[10]). Insomma, anche se quello televisivo è tuttora il mezzo di informazione più diffuso nel Paese, non tenere all'interno della riflessione il contesto digitale sarebbe anacronistico. Tenendo presente che un altro elemento che influisce sulla modalità di attuazione della disciplina è quello del sistema elettorale adottato, e dunque del modo in cui i partiti si organizzeranno in vista della competizione elettorale[11].
In questo contesto, ragionare sulla disciplina relativa alla *par condicio* risulta necessario, trattandosi di un insieme di disposizioni che riflette un "imperativo costituzionale", ma che al contempo necessita per l'appunto di modifiche ed aggiornamenti.

2. Lo stato dell'arte: cenni alla regolamentazione della *par condicio*

Parlare di *par condicio* può suonare per certi versi anacronistico: il tema sembra appartenere a un periodo storico per la verità non così risalente nel tempo, ma che pare distante per via dei profondi mutamenti (principalmente tecnologici, ma anche concernenti il contesto politico e il sistema dei partiti) che sono intervenuti nei primi due decenni degli anni 2000. L'entrata in vigore della relativa legge infatti risale al 2000 – l. 28/2000 – e risponde a esigenze sollevate da un contesto tecnologico e politico-economico ben diverso da quello attuale, al pari della rilevante pronuncia in materia della Corte costituzionale – Corte cost. 7 maggio 2002, n. 155 – che più di venti anni fa ha affermato come il rispetto della *par condicio* risponda all'«imperativo costituzionale»[12] di assicurare il corretto svolgimento del confronto politico, pietra angolare dei sistemi democratici.
L'attuale disciplina consta di due "tronchi", che si fondano sulla distinzione di cui all'art. 5[13] tra programmi di informazione e programmi di comunicazione politica: con riferimento ai primi, la disciplina si occupa dell'accesso ai mezzi di informazione in tempo di campagna elettorale o referendaria, quanto ai secondi viene disciplinata la comunicazione politica *tout court*.
Rinviando a lavori più estesi per un'analisi storica e organica della disciplina[14], nonché

[10] Sul concetto di "disintermediazione", cfr. tra gli altri, P. Stringa, *Che cos'è la disintermediazione*, Roma, 2017; V. Satta-S. Gonario, *Disintermediazione*, in G. Formigoni-L. Caimi (a cura di), *Dizionarietto di politica. Le nuove parole*, Brescia, 2022, 138 ss.; in particolare, con riferimento al legame tra disintermediazione e formazione del consenso elettorale, cfr. M. Ladu, *La costruzione del consenso politico-elettorale e l'utilizzo dei social media nel tempo della "disintermediazione democratica"*, in *federalismi.it*, 23, 2022, spec. 197 ss.; riguardo alla comunicazione politica e al ruolo di "mediatori" svolto dai *social network*, cfr. R. Rega-L. Parisi, *La comunicazione degli attori politici: tra disintermediazione e media sociali*, in E. Cioni-A. Marinelli (a cura di), *Le reti della comunicazione politica. Tra televisione e social network*, Firenze, 2010, e E. Amaturo-G.M. Padricelli-G. Punziano, *I volti e le parole: nuove frontiere nella disintermediazione della politica*, in *Sociologia e ricerca generale*, 131, 2023, 63 ss.

[11] Se ne parlerà in relazione al caso del (mancato) confronto televisivo tra Giorgia Meloni ed Elly Schlein del maggio del 2024 (v. *infra*, par. III), e in termini generali *infra*, par. 4.

[12] Corte cost., 7 maggio 2002, n. 155, par. 2 del "considerato in diritto".

[13] Di cui si dirà più estesamente *infra*, par. 2.1.

[14] Si rinvia, tra gli altri, a E. Bettinelli, *Par condicio*, cit.; M.R. Allegri, *Oltre la par condicio. Comunicazione politico-elettorale nei social media, fra diritto e autodisciplina*, Milano, 2020.

dell'estendibilità della stessa – che ha ad oggetto prevalentemente il mezzo televisivo, ed in particolare la televisione generalista, con alcune disposizioni più specifiche per le tv locali e per la stampa – a tutti i mezzi di comunicazione[15], è comunque necessario richiamarne brevemente alcuni punti essenziali, o quantomeno risalire agli obiettivi che questa si pone. In via generale la materia della comunicazione politica è regolata dalla l. 212/1956 (come modificata dalla l. 130/1975 e dal d.l. 107/1984, convertito in l. 10/1985[16]), dalla l. 103/1975 (che ha istituito la Commissione parlamentare bicamerale per gli indirizzi generali e la vigilanza sul servizio pubblico radiotelevisivo, tutt'ora in essere quale mezzo di indirizzo e controllo da parte del Parlamento nei confronti della radiotelevisione pubblica), dalla l. 515/1993[17] (che sanciva il principio della parità di *chances* in campagna elettorale, con riferimento dunque al concetto di propaganda politico-elettorale[18], che in un contesto liberaldemocratico non può distorcersi in attività occulta o manipolatoria[19], introducendo un sistema di vigilanza dualistico Commissione parlamentare - AGCOM tuttora in vigore[20]), e, in ultimo, dalla citata l. 28/2000[21]. L'obiettivo della disciplina è sintetizzabile in questi termini: imporre a tutte le emittenti radiotelevisive – sia pubbliche che private – di concedere identico spazio alle formazioni politiche per la diffusione delle proprie idee, opinioni e letture della realtà, improntando l'intero sistema dell'informazione e della comunicazione politica a criteri di eguaglianza, equità e trasparenza, specie – come stabilito dall'art. 1 l. 28/2000 – in tempo di campagna elettorale. A ciò si aggiungono il divieto di pubblicare sondaggi politico-elettorali nei quindici giorni precedenti alla data del voto (art. 8) e il divieto per le reti di rilevanza nazionale di trasmettere messaggi di propaganda politica a pagamento (art. 9).

Va altresì ricordato che la Corte costituzionale – con la citata decisione Corte cost. 24 aprile 2002, n. 155 – oltre ad aver rigettato le questioni di legittimità sollevate in relazione a diverse disposizioni contenute nella l. 28/2000[22] per contrasto con gli artt. 3, 21 e 42 Cost., ha ritenuto la legge in questione "costituzionalmente necessaria", o comunque di «attuazione costituzionale»[23], in quanto volta ad assicurare che le forze po-

---

15 Si v. in particolare O. Grandinetti, *La par condicio al tempo dei social, tra problemi "vecchi" e "nuovi", ma, per ora, tutti attuali*, in questa *Rivista*, 3, 2019, 104 ss.; M.R. Allegri, *Oltre la par condicio*, cit., 81-82, secondo cui è "sorprendente" l'assenza di regole specifiche sul punto.

16 Che ha esteso la disciplina del silenzio elettorale di cui all'art. 9 l. 212/1956, anche ai mezzi radiotelevisivi.

17 Per una più estesa analisi della legge in questione si rinvia al già citato M.R. Allegri, *Oltre la par condicio*, cit., 90-93.

18 Si rinvia, per una ricostruzione del concetto, a F. Lanchester, *La propaganda elettorale (e referendaria) in Italia*, cit., 1996.

19 M. Gobbo, *La propaganda politica nell'ordinamento costituzionale*, Padova, 1997, 69.

20 La distinzione è tra servizio pubblico radiotelevisivo, sottoposto alla vigilanza della Commissione parlamentare, e diversi mezzi di comunicazione gestiti da soggetti privati, sorvegliati dall'AGCOM.

21 È interessante notare come ogni disciplina risponda a problematiche differenti di volta in volta sollevata dal contesto sociale, politico, tecnico e culturale del tempo. Si rinvia a riguardo a G.E. Vigevani, *I media di servizio pubblico nell'età della rete*, Torino, 2018, e M.R. Allegri, *Oltre la par condicio*, cit., spec. 83-101.

22 Si trattava, nello specifico, degli artt. 1, 2, 3, 4, 5, e 7.

23 R. Zaccaria, *Presente e futuro della par condicio*, in M. Manetti, R. Borrello (a cura di), *Il diritto*

litiche possano prendere parte alle competizioni elettorali in condizioni di eguaglianza, e che di conseguenza i cittadini possano accedere ad un'informazione il più possibile plurale ed imparziale. La disciplina sulla parità di trattamento consisterebbe in tal senso un dispositivo di salvaguardia necessario per tutelare la forma di Stato democratica-costituzionale, in quanto colmerebbe un *vulnus* alla tutela di diritti fondamentali, nonché al buon funzionamento della democrazia. Detto altrimenti, la disciplina, come si evince dal preambolo e dai lavori preparatori, ha quantomeno due finalità: evitare trattamenti diseguali o irragionevoli in materia di comunicazione politica (e di informazione, limitatamente ai periodi elettorali), ma anche garantire ai cittadini l'accesso a un'informazione quanto più possibile rispondente ai criteri del pluralismo interno, nonché esaustiva e completa, così da evitare condizionamenti indebiti e tutelare la libertà di voto garantita dall'art. 48 Cost., che riguarda anche la sua fase preparatoria[24].

2.1. Il ruolo dell'AGCOM (rinvio)

In tema di sorveglianza e controllo sul rispetto della disciplina in materia di informazione e comunicazione politica un ruolo centrale è affidato all'Autorità per le garanzie nelle comunicazioni (nota con l'acronimo "AGCOM").
È stata la l. 249/1997 (recante l'"Istituzione dell'Autorità per le garanzie nelle comunicazioni e norme sui sistemi delle telecomunicazioni e radiotelevisivo"), ad affidare ad un'apposita autorità – l'AGCOM, per l'appunto – la «tutela e la garanzia dei principi in materia di pluralismo dell'informazione e di correttezza, completezza, imparzialità, obiettività, lealtà dell'informazione e di apertura alle diverse opinioni e tendenze politiche»[25].
L'AGCOM è composta da un Presidente, due Commissioni (la Commissione per le infrastrutture e le reti e la Commissione per i servizi e i prodotti) e dal Consiglio, e «al pari delle altre Autorità previste dall'ordinamento italiano, […] risponde del proprio operato al Parlamento»[26]. I quattro commissari – originariamente erano otto, dimezzati dal d.l. 201/2011, cd. "Decreto Salva Italia" – sono eletti dal Parlamento (due dalla Camera dei Deputati, due dal Senato della Repubblica), a scrutinio segreto, e restano in carica sette anni. Il Presidente dell'Autorità viene nominato mediante decreto del Presidente della Repubblica, su proposta del Presidente del Consiglio dei ministri e in accordo con il Ministro dello Sviluppo economico. Il nominativo indicato dal Presidente del Consiglio dei ministri deve essere preliminarmente sottoposto al parere delle Commissioni parlamentari competenti[27], che si pronunciano con una maggioranza

dell'informazione, temi e problemi, Modena, 2019, 223 ss.

[24] Per un'analisi del requisito della libertà del voto in tale fase si rinvia a C. Mortati, *Istituzioni di diritto pubblico*, Padova, 1952, 43; F. Lanchester, *Voto (diritto di)*, in *Enciclopedia del Diritto*, Milano, vol. 46, 1989, 1112 ss.; L. Paladin, *Diritto Costituzionale*, Padova, 1991, 292; P. Barile, *Istituzioni di Diritto Pubblico*, Padova, 1991, 151 ss.; E. Grosso, *Art. 48*, cit., 962.

[25] L. 249/1997.

[26] Come si evince dal sito *web* della stessa Autorità, *AGCOM.it*, alla voce "Istituzione".

[27] Ai sensi dell'art. 2 della l. 481/1995.

qualificata dei due terzi dei loro membri[28].

La citata legge istitutiva dell'AGCOM ha individuato le competenze dell'Autorità in tema di propaganda, pubblicità e informazione politica in termini generali, senza far cioè riferimento ad alcun mezzo di comunicazione in particolare (mentre la successiva l. 28/2000, come si vedrà[29], ha invece previsto un ruolo dell'Autorità specificamente per la comunicazione politico-elettorale con riferimento al mezzo radiotelevisivo)[30].

L'Autorità si autodefinisce come "Autorità convergente", che «svolge funzioni di regolamentazione e vigilanza nei settori delle comunicazioni elettroniche, dell'audiovisivo, dell'editoria, delle poste e più recentemente delle piattaforme *online*»[31]. La Commissione per i servizi e per i prodotti «garantisce l'applicazione delle disposizioni vigenti sulla propaganda, sulla pubblicità e sull'informazione politica nonché l'osservanza delle norme in materia di equità di trattamento e di parità di accesso nelle pubblicazioni e nella trasmissione di informazioni e di propaganda elettorale ed emana le norme di attuazione»[32]. Il Consiglio, inoltre, ha il compito di accertare la sussistenza di posizioni dominanti nel settore radiotelevisivo, e di adottare i relativi provvedimenti[33], nonché di accertare la mancata attuazione da parte dell'emittente radiotelevisiva di servizio pubblico delle linee di indirizzo formulate dalla Commissione parlamentare per l'indirizzo generale e la vigilanza dei servizi radiotelevisivi.

Ciò detto, è utile tentare di comprendere come l'Autorità intenda il proprio ruolo in tema di informazione e comunicazione politica. Nel 2002 (Corte cost. 24 aprile 2002, n. 155)[34], con una decisione relativa alla legittimità costituzionale della l. 28/2000, la Corte costituzionale, rifacendosi alla distinzione tra programmi di "informazione" e di "comunicazione politica", ha individuato due capisaldi in materia, che devono essere congiuntamente rispettati: un primo di carattere generale, secondo cui non è possibile imporre ai programmi di informazione televisiva dei «limiti […] che derivino da moti-

[28] Tale parere, esplicitamente richiesto dalla norma, è da considerarsi obbligatorio e vincolante, poiché la legge stabilisce che le nomine non possono essere effettuate in assenza di un parere favorevole delle Commissioni parlamentari.

[29] V. *infra*, par. 3.

[30] Alla luce dei principi enunciati dal Testo Unico dei servizi di media audiovisivi e radiofonici (d.lgs. 177/2005) che, tra le altre cose, qualifica l'informazione come servizio di interesse generale (art. 7, par. 1), ed individua l'obiettività, l'imparzialità, la completezza e la lealtà dell'informazione quali principi fondamentali che informano l'intera materia, l'AGCOM ha ritenuto che la propria funzione si concretizzasse, pur in assenza di una previsione espressa, nell'«esercizio di un ruolo di impulso e di coordinamento tra i diversi attori operanti nel settore dell'informazione *online* per favorire l'autoregolamentazione su base volontaria ai fini di contrasto dei fenomeni di disinformazione *online*» (Delibera 423/17/CONS, "Istituzione di un tavolo tecnico per la garanzia del pluralismo e della correttezza dell'informazione sulle piattaforme digitali", con cui l'Autorità ha altresì istituito un "Tavolo tecnico per la garanzia del pluralismo e della correttezza dell'informazione sulle piattaforme digitali").

[31] Sito *web* AGCOM, *AGCOM.it*, alla voce "Istituzione"; con riferimento al ruolo svolto dall'Autorità in relazione alle piattaforme digitali, cfr. M. Giannelli, *Poteri dell'AGCOM e uso degli algoritmi. Tra innovazioni tecnologiche ed evoluzioni del quadro regolamentare*, in *Osservatorio sulle fonti*, vol. 2, 2021, 859 ss.

[32] Art. 1, lett. *b)*, par. 9 l. 249/1997.

[33] E. Albanesi-A. Valastro-R. Zaccaria, *Diritto dell'informazione e della comunicazione*, Padova, 2016, 158-162, che fa altresì notare come tale prerogativa sia stata realizzata "timidamente" dall'Autorità stessa.

[34] Su cui si tornerà *infra*, par. 3.

vi connessi alla comunicazione politica»[35] *(i)*; e un secondo di carattere particolare, per il quale è possibile limitare le trasmissioni di informazione solo qualora tali limitazioni siano volte a «prevenire in ogni modo qualsiasi influenza, anche in forma surrettizia, sulle libere e consapevoli scelte degli elettori, in momenti particolarmente delicati della vita democratica del Paese»[36]. Tali limitazioni, ai sensi dell'art. 5 c. 1 l. 28/2000, sono peraltro circoscritte ai soli periodi elettorali per quanto riguarda le emittenti radiotelevisive private, e, al di fuori di tale specifico periodo, sottintendono la «massima espansione della libertà di manifestazione del pensiero per le emittenti private»[37].

Secondo la Corte sarebbe dunque necessario operare due distinzioni: una tra il differente ruolo svolto da emittenti pubbliche ed emittenti private nella garanzia del pluralismo *(i)*, e un'altra tra trasmissioni di informazione in senso lato e trasmissioni di comunicazione politica (come espressamente previsto dalla stessa legge sulla *par condicio*) *(ii)*.

L'AGCOM, sulla base delle già indicate competenze, ha assunto un orientamento differente, distaccandosi di fatto dalla pronuncia della Corte del 2002 e superando tale duplice distinzione.

Quanto al primo profilo, l'Autorità garante[38], richiamandosi alla l. 223/1990 (cd. legge "Mammì") ha optato per una «considerazione unitaria dell'attività radiotelevisiva come servizio pubblico, connotata da vincoli permanenti in tema di indipendenza, obiettività e completezza, sia per i soggetti pubblici che per quelli privati»[39];

Con riferimento al secondo punto, i criteri a cui l'Autorità si rifà per valutare se un'attività comunicativa rientri nell'alveo dell'informazione o in quello della comunicazione politica tendono ad essere labili e poco chiari, tanto da condurre non tanto ad una «necessaria distinzione», quanto ad una «assimilazione»[40] delle due categorie.

Richiamandosi altresì ad una pronuncia del Consiglio di Stato sul punto[41], ciò si è tradotto in una applicazione generalizzata, da parte di AGCOM, del criterio quantitativo del tempo di parola quale principale parametro per assicurare il rispetto della parità di trattamento tra i soggetti politici impegnati in una competizione elettorale[42]. In altre parole, assottigliando le suddette distinzioni, si l'Autorità è finita per applicare un concetto di rispetto del pluralismo basato sul conteggio *tout court* delle presenze televisive, senza far riferimento al contesto in cui queste presenze si concretizzano; concetto che pare distanziarsi dalla parità di trattamento ex art. 5 c. 1 l. 28/2000, che riguarderebbe

35 Ai sensi dell'art. 2 c. 2 l. 28/2000.

36 Corte cost. 24 aprile 2002, n. 155.

37 R. Borrello, *La par condicio nella campagna elettorale delle elezioni politiche del 25 settembre 2022: profili generali e alcuni casi specifici*, in *Nomos. Le attualità del diritto*, 3, 2022, 5.

38 AGCOM, delibera 90/03/CSP; AGCOM, delibera 91/03/CSP.

39 R. Borrello, *La par condicio nella campagna elettorale*, cit., 6; si v. anche R. Borrello-A. Frosini, *La disciplina delle trasmissioni radiotelevisive di rilievo politico in Italia*, vol. I, *Premesse generali e di diritto comparato – La disciplina dei periodi ordinari*, Rimini, 2019, 141 ss.

40 R. Borrello, *La par condicio nella campagna elettorale*, cit., 6-7.

41 Cons. Stato, sez. III, 10 dicembre 2014, n. 6067.

42 Con riferimento alle elezioni politiche del 2022, la CIVS (CIVS, delibera 18/2022) adotta il criterio delle presenze dei soggetti politici nelle trasmissioni televisive quale criterio per assicurare il rispetto della parità di trattamento nel periodo elettorale.

il divieto di esclusione di uno o più parti politiche nel trattare una determinata notizia o un determinato tema, comportando cioè un'esclusione delle stesse e dunque un irragionevole trattamento differente di situazioni uguali[43].

3. La disciplina della *par condicio* "in azione": il mancato confronto televisivo Meloni-Schlein

Un caso che pone interrogativi circa l'attualità della disciplina sulla *par condicio* è quello relativo alla decisione (o meglio, del parere) dell'AGCOM che ha portato (indirettamente) alla cancellazione del confronto televisivo tra Giorgia Meloni (Presidente del Consiglio dei ministri e *leader* di "Fratelli d'Italia") ed Elly Schlein (segretaria del "Partito Democratico", la più rappresentativa delle forze politiche di opposizione) che si sarebbe dovuto tenere nel corso della trasmissione televisiva "Porta a porta", in onda su Rai 1 il 23 maggio 2024, in vista delle elezioni europee dell'8 e 9 giugno successivi[44]. "L'intervento è perfettamente riuscito, il paziente è morto", è la battuta che sorge spontanea all'esito della vicenda: la *par condicio* è stata fatta salva, ma il dibattito pubblico ne è uscito impoverito. L'intervento dell'Autorità non ha negato di per sé la possibilità che il confronto si svolgesse, ma, rimettendo la decisione alla maggioranza delle forze politiche coinvolte nella competizione elettorale, ha di fatto condotto alla cancellazione dello stesso.

Nel caso di specie, all'esito della riunione del 15 maggio 2024, il Consiglio dell'Autorità per le Garanzie nelle Comunicazioni si è pronunciato sulle specifiche richieste provenienti dall'emittente pubblica RAI, nonché sulla comunicazione della Presidente della Commissione parlamentare per l'indirizzo generale e la vigilanza dei servizi radiotelevisivi (la senatrice Barbara Floridia), e sulla segnalazione del giornalista Michele Santoro, in ordine all'organizzazione di confronti televisivi tra diversi esponenti politici in vista delle elezioni europee previste per l'8 e il 9 giugno successivi.

Richiamandosi alla disciplina sulla *par condicio*[45], ed in particolare ad AGCOM, delibera 90/24/CONS "Disposizioni di attuazione della disciplina in materia di comunicazione politica e di parità di accesso ai mezzi di informazione relative alla campagna per l'elezione dei membri del Parlamento europeo spettanti all'Italia fissata per i giorni 8 e 9 giugno 2024", e al provvedimento del 9 aprile 2024 della Commissione parlamentare per l'indirizzo generale e la vigilanza dei servizi radiotelevisivi[46], l'Autorità ha

[43] R. Borrello, *La par condicio nella campagna elettorale*, cit., 12 che fa riferimento al "giochino dell'elastico" (così definito da A. Fontanarosa, *Lasorella (AGCOM): "La par condicio va estesa anche a web e social"*, (intervista al Presidente AGCOM, in *Repubblica.it*, 24 settembre 2022, che «consentirebbe di favorire determinate forze politiche, dando nei notiziari alta visibilità alle forze politiche non gradite, nella prima parte della campagna elettorale, per poi, sulla base dell'inevitabile ordine di riequilibrio da parte dell'AGCOM, poter dare visibilità "compensativa" più elevata ai propri favoriti, nella più "pregiata" fase di campagna, più vicina al momento del voto.

[44] AGCOM, Comunicato stampa del 15 maggio 2024.

[45] Non richiamando, tuttavia, la legge sulla *par condicio* (l. 28/2000).

[46] Secondo cui la RAI e le emittenti private nazionali che vogliano trasmettere confronti elettorali «devono assicurare una effettiva parità di trattamento tra tutti i predetti esponenti […] oltre che nell'ambito della medesima trasmissione, anche nell'ambito di un ciclo di più trasmissioni dello

individuato quale finalità del proprio agire la valutazione del rispetto del principio di parità di trattamento, che nel caso di specie «può essere garantit[o] dall'offerta a tutti i soggetti politici della medesima opportunità di confronto»[47]. Si è pertanto ipotizzata l'organizzazione di una serie di confronti televisivi a coppie tra i diversi rappresentanti delle forze politiche coinvolte nella competizione elettorale, nella medesima fascia oraria e per la medesima durata temporale. Dal principio di parità di trattamento l'Autorità ha altresì fatto discendere che le trasmissioni televisive destinate al dibattito tra attori politici concorrenti nella medesima competizione elettorale «possano considerarsi legittime ove il relativo *format* sia accettato da una larga maggioranza delle liste in competizione elettorale e comunque dalla maggioranza delle liste con rappresentanza in Parlamento»[48]. Se lo "schema" non avesse ricevuto tale "*placet*", allora l'intero "pacchetto" di incontri sarebbe stato cancellato.
Inoltre, qualora alcune parti politiche coinvolte nella competizione elettorale avessero rinunciato, o comunque si fossero dette contrarie, al suddetto *format*, le medesime emittenti avrebbero dovuto prevedere degli appositi "spazi compensativi", per rispettare la suddetta normativa e il principio di pari opportunità di ascolto.
Traducendo in termini "numerici" il parere reso dall'Autorità, se cinque liste su otto si fossero dette d'accordo il confronto Meloni-Schlein si sarebbe potuto effettivamente tenere; al netto della vaghezza che connota l'eventuale assenso delle liste rappresentate in Parlamento cui era subordinata la "fattibilità" del dibattito (in che forma, e da chi, deve essere espresso tale assenso, e in caso di silenzio cosa avviene?), quattro *leader* delle forze politiche in gioco hanno rigettato il *format* proposto da AGCOM[49], per cui il confronto televisivo è stato annullato.

3.1. Una decisione discussa

Il parere richiamato ha ricevuto parere discordanti. Va premesso che l'AGCOM già nel 2022 (AGCOM, delibera 304/22/CONS, "Richiamo alla corretta applicazione dei principi a tutela del pluralismo e della parità di trattamento nei confronti radiotelevisivi trasmessi nei programmi di informazione durante la seconda fase della campagna per le elezioni della Camera dei deputati e del Senato della Repubblica fissate per il giorno 25 settembre 2022"), ha di fatto[50] considerato "Porta a Porta" un programma di comunicazione politica in senso stretto (applicando l'art. 4 c. 2 lett. *b)* l. 28/2000)[51], applicando dunque le regole in materia di *par condicio* proprie della comunicazione

stesso programma, organizzate secondo le stesse modalità e con le stesse opportunità di ascolto», cfr. Comunicato stampa AGCOM del 15 maggio 2024.

47 AGCOM, comunicato stampa del 15 maggio 2024, cit.

48 *Ibid.*

49 Lo ha comunicato la stessa Rai, *Rai, salta il confronto Meloni-Schlein: non c'è la maggioranza chiesta dall'AGCOM*, in *Rainews*, 16 maggio 2024.

50 Richiamando solo formalmente la normativa per i programmi di carattere informativo e di approfondimento.

51 R. Borrello, *La par condicio nella campagna elettorale*, cit., 11.

politica.
Con riferimento al parere sul dibattito Meloni-Schlein si registrano sia posizioni e motivazioni favorevoli alla decisione cui è pervenuta l'Autorità, che altre maggiormente critiche. Non è detto – lo si vedrà "tirando le fila" del discorso – che i due "poli" non possano coesistere: si tratta infatti di una materia segnata da un elevato grado di complessità e che coinvolge molteplici beni costituzionalmente rilevanti, per cui le analisi e le piste di ragionamento proposte non possono che tener conto di tali complessità e connaturate ambiguità, non giungendo obbligatoriamente a letture univoche o monodirezionali.

3.1.1. Osservazioni favorevoli

È stato fatto notare che parere reso dall'AGCOM in data 15 maggio 2024 presenta alcuni aspetti di ragionevolezza[52]. La soluzione prospettata risulterebbe infatti condivisibile, quantomeno nella parte iniziale: il confronto televisivo Meloni-Schlein può tenersi, a patto che si realizzino altri "duelli" – il termine, largamente utilizzato specie in ambito giornalistico, non convince, specie nel contesto di un sistema elettorale proporzionale – televisivi tra gli altri *leader* esclusi, o che si dia comunque la possibilità alle altre forze politiche coinvolte di rilasciare un'intervista della medesima durata, così da garantire parità di trattamento e un contraddittorio (diretto o indiretto) alle forze politiche in competizione elettorale. Può ritenersi che il *format* proposto rappresenti un punto di equilibrio sensato e concretamente raggiungibile, in grado cioè di tenere insieme le diverse istanze apparentemente confliggenti.
La soluzione intercetta poi un interrogativo teorico e di sistema: può, in un contesto proporzionale, prevedersi una contrapposizione tra soli due *leader*, seppur siano quelli maggiormente rappresentativi nel Paese? È una tale prospettiva compatibile con la disciplina sulla *par condicio* precedentemente richiamata[53]? I dibattiti tra due *leader* politici sono propri del contesto americano, e sono stati in qualche misura "recepiti" nel contesto italiano a partire dal "passaggio" al sistema maggioritario (dal 1993/94, e, in maniera ancor più chiara, dal 1996 in poi)[54]. La legge italiana sulla *par condicio* si basa infatti sul modello francese[55], che, come noto, risponde a logiche proprie di una forma di governo differente[56]. Per eleggere il Parlamento europeo viene invece utilizzato un

[52] A. Nicita, *Intervista sulla delibera dell'AGCOM sul confronto televisivo tra Elly Schlein e Giorgia Meloni*, in *Radio radicale*, 17 maggio 2024.

[53] V. *supra*, par. 3.

[54] L. 276/1993 (cd. "*Mattarellum*").

[55] Sulle radici francesi della disciplina sulla *par condicio* e per un'analisi comparata della disciplina si rinvia a M. P. Caruso, *La "par condicio" in Francia, Germania, Regno Unito e Spagna. Linee guida di analisi comparata*, in *Comunicazione politica,* vol. 1, 2000.

[56] In cui si svolgono elezioni presidenziali con doppio turno, e i confronti tra i rappresentanti dei due "poli" contrapposti hanno un valore informativo importante. Per un'analisi del sistema francese si rinvia, tra gli altri, a A. Di Giovine-A. Algostino-F. Longo-A. Mastromarino, *Lezioni di diritto costituzionale comparato*, Milano, 2017, spec. cap. XVI.

sistema elettorale di tipo proporzionale con voto di preferenza[57], con la sola previsione di una soglia di sbarramento del 4%. La logica è chiara: essendo il Parlamento europeo l'organo rappresentativo per eccellenza all'interno dell'Unione Europea, dotato di competenze legislative, di vigilanza e bilancio[58], ed essendo dunque un luogo in cui ciò che più conta è la discussione e il confronto anziché la necessità di assumere decisioni in modo stabile e celere, lo stesso deve il più possibile rappresentare tutte le diverse "anime" politiche presenti nei vari Stati membri[59].

Lo schema di confronti proposto dall'AGCOM costituirebbe un tentativo – per certi versi ben riuscito, seppur complesso – di applicare la disciplina sulla parità di trattamento a un modello comunicativo proprio delle logiche maggioritarie, adattandolo a un contesto puramente proporzionale.

Un ulteriore argomento in linea con il parere reso dell'AGCOM è quello che considera, in accordo con la Corte costituzionale, la legge sulla *par condicio* ancora un imperativo costituzionale (secondo la già citata Corte cost. 7 maggio 2002, n. 155), non immodificabile nei metodi, bensì nella sostanza, in quanto precipitato diretto della forma di Stato democratica[60]. Ci sarebbe, insomma, un argomento di carattere giuridico-costituzionale, che ragiona a partire dai principi che stanno alla base della normativa richiamata dall'AGCOM nella sua decisione, che supporterebbe la soluzione proposta dall'Autorità. Il *format* rispetterebbe infatti la parità di trattamento in tema di comunicazione politica e i principi della relativa disciplina[61], che in un contesto democratico non può essere ignorata né aggirata.

Permangono tuttavia alcuni dubbi non agevolmente superabili sulla decisione, quali la sottoposizione dello schema di confronti televisivi alla maggioranza delle liste rappresentate all'interno del Parlamento europeo o comunque partecipanti alla competizione elettorale europea.

3.1.2. Osservazioni contrarie

Il parere AGCOM del 15 maggio 2024 ha per l'appunto altresì sollevato diversi interrogativi, nonché alcune critiche e perplessità. C'è *in primis* un elemento di carattere ideologico, di stampo prettamente liberale, secondo cui i pubblici poteri non dovrebbero indebitamente intromettersi nella regolamentazione del discorso pubblico. Lungi dal lasciare un compito così cruciale per la sopravvivenza una democrazia privo di presidi

[57] Contenuto in Italia nella l. 18/1979, come modificata dalla l. 10/2009, che ha introdotto la soglia di sbarramento.

[58] Lo riporta la stessa pagina *web* istituzionale del Parlamento europeo (*europarl.europa.eu*), alla voce "*legislative powers*".

[59] Sul funzionamento e le competenze del Parlamento europeo, e i relativi limiti relativi ai poteri di intervento e di "incidenza", si rinvia a N. Lupo-A. Manzella, *Parlamento europeo*, in R. Bifulco-A. Celotto-M. Olivetti (a cura di), *Digesto delle discipline pubblicistiche*, Torino, 285 ss.

[60] G.E. Vigevani-M. Cazzaniga, *Comunicazione politica e Costituzione tra televisione e piattaforme digitali*, in questa *Rivista*, 1, 2024, 15.

[61] L'AGCOM considera "Porta a Porta" un programma di comunicazione politica e non di informazione, v. *infra, par.* 3.

o limitazioni, sarebbe opportuno lasciare alla libera stampa il diritto – ma anche il dovere – di costruire i prodotti informativi che reputa più adatti e utili al pubblico, che resta libero, qualora non voglia "scegliere" quello specifico "prodotto", di sceglierne altri, all'interno del *free marketplace of ideas*[62]. Non si ritiene, insomma, che Autorità pubbliche possano decidere chi, e sulla base di quali criteri, possa o meno partecipare a un dibattito giornalistico dentro un programma tv.

Tale tesi sarebbe corroborata anche da un elemento "di risultato". Affidando l'applicazione della disciplina sulla *par condicio* ad Autorità pubbliche e non all'autonomia dei mediatori qualificati dell'informazione, l'esito è quello di un impoverimento dell'informazione, come testimoniato dal caso in esame: il dibattito Meloni-Schlein non si è tenuto, e il discorso pubblico, lungi dall'essere salvaguardato, ne è uscito indebolito. Secondo tale visione, un ruolo centrale nella strutturazione dell'informazione sarebbe insomma da attribuire all'autonomia dei giornalisti e dei soggetti editoriali, al riparo dalle interferenze del decisore pubblico[63]. Se una delle finalità della l. 28/2000 è di tipo informativo – «promuove[re] […] l'accesso ai mezzi di informazione per la comunicazione politica»[64] –, ovvero favorire e incentivare la partecipazione e la diffusione del discorso pubblico, il parere in esame non sembra aver raggiunto l'obiettivo. Va però fatto notare. Che AGCOM non ha di per sé vietato lo svolgimento del dibattito, bensì ha previsto strumenti compensativo e rimesso la decisione alle forze politiche in gioco. Inoltre, non può farsi a meno di tenere in considerazione il fatto che la decisione dell'Autorità Garante per le Comunicazioni sembri per certi versi anacronistica: in un contesto in cui l'informazione è di fatto segnata da una inedita facilità di accesso generalizzato[65], e non incontra di per sé limiti quantitativi né regolamentazioni stringenti nell'ecosistema digitale[66], vietare lo svolgimento di un dibattito tra due esponenti poli-

[62] La metafora, utilizzata dal giudice statunitense O. Holmes nella *dissenting opinion* del caso *Abrams vs. United States*, 1919, è diventata centrale nella riflessione in materia (essendo per certi versi travisata rispetto all'intento originario, inscritto in un contesto profondamente diverso). Per diverse analisi sul ruolo del free markeplace nel contesto attuale si rinvia a V. Visco Comandini, *Le fake news sui social network: un'analisi economica*, in questa *Rivista*, 2, 2018, A. Nicita, *Il mercato delle verità*, Bologna, 2021 M. Bassini, *Internet e libertà di espressione. Prospettive costituzionali e sovranazionali*, Canterano, 2019; M. Bassini-G.E. Vigevani, *Primi appunti su fake news e dintorni*, in questa *Rivista,* 1, 2017, O. Pollicino, *General report: freedom of speech and the regulation of fake news*, Cambridge, 2023.

[63] Affonda le radici in quella visione per cui le regole poste a tutela della libertà di informazione nascano e siano tuttora posta principalmente per evitare che il potere pubblico interferisca con la libertà di manifestazione del pensiero (cfr., in tal senso, G.E. Vigevani, *Sistema informativo e opinione pubblica nel tempo della pandemia*, in *Quaderni Costituzionali*, 4, 2020, 779 ss. Tale visione solleva altresì alcune perplessità sulla citata composizione dell'AGCOM (v. *supra*, par. 2).

[64] Art. 1 l. 28/2000.

[65] Sia per ricevere che per produrre l'informazione; sulla facilità di accesso alla rete, cfr. M. Orofino, *L'inquadramento costituzionale del web 2.0: da nuovo mezzo per la libertà di espressione a presupposto per l'esercizio di una pluralità di diritti costituzionali*, in AA.VV., *Da Internet ai social network*, Santarcangelo di Romagna, 2013; G. Azzariti, *Internet e Costituzione*, in *Costituzionalismo.it*, 3, 2011, 374 ss; G. De Minico, *Accesso a Internet tra mercato e diritti sociali nell'ordinamento europeo e nazionale*, in G. De Minico (a cura di), *Libertà in rete, libertà dalla rete*, Torino, 2020, 209 ss.; cfr. anche S. Rodotà, *Verso una dichiarazione dei diritti di internet*, in *Camera.it*, 24 novembre 2014, che annovera il diritto di accesso a *internet* tra i diritti sociali fondamentali dell'individuo *ex* art. 2 Cost..

[66] Sul tema della regolamentazione delle piattaforme, nonché della loro responsabilità editoriale, la riflessione giuridica, sia nel contesto europeo che in quello continentale, è in rapida evoluzione; si rinvia, per tutti, a G. Pitruzzella, O. Pollicino-S. Quintarelli, *Parole e potere. Libertà d'espressione, hate speech e fake*

tici in diretta televisiva può sembrare una misura ininfluente, o comunque facilmente aggirabile. Basterebbe che il confronto televisivo si fosse tenuto in diretta *streaming*, su YouTube, su qualunque altro *social media* o anche negli spazi predisposti da qualsiasi quotidiano italiano *online* perché potesse essere pienamente legittimo. Insomma, seppur possono anche ritenersi condivisibili i principi che informano la disciplina sulla *par condicio* e le altre disposizioni richiamate dall'AGCOM per motivare la propria decisione, rimarrebbe un insuperabile elemento di fatto: è insensato applicare una disciplina così stringente per le trasmissioni televisive, quando la medesima disciplina non trova applicazione alcuna con riferimento ad altri mezzi di informazione, la cui diffusione è peraltro in crescita. Bisogna però al contempo tenere presente il fatto che la televisione sia saldamente il mezzo informativo più utilizzato nel Paese[67], e che gode ancora di una certa presunzione di affidabilità. Non è detto, dunque, che negare la possibilità di svolgere il dibattito in diretta televisiva in prima serata su Rai 1 sia una decisione del tutto priva di effetti, o comunque superabile "dirottandolo" su un altro mezzo di informazione nella convinzione di ottenere risultati equivalenti in termini di diffusione ed influenza sull'opinione pubblica.

Se si è detto che non mancano le argomentazioni per considerare la soluzione prospettata dall'AGCOM ragionevole nella prima parte – quella che propone uno schema di confronti tra i vari partiti politici coinvolti nella competizione elettorale[68] –, la scelta di subordinare l'applicabilità di tale schema alla maggioranza dei partiti convincerebbe meno: si offre di fatto la strutturazione di un *format* di informazione pubblica alle strategie politico-elettorali dei partiti, i quali, sulla base di considerazioni e strategie volte – legittimamente – al proprio interesse valutano se tale organizzazione del discorso pubblico sia o meno favorevole rispetto alla propria campagna, e sulla base di ciò hanno la possibilità di decidere se l'intero *format* debba tenersi o meno. Posto che il parere dell'AGCOM è espressamente finalizzato a garantire una parità di trattamento tra i soggetti coinvolti, e dunque ad assicurare una pari visibilità a chi altrimenti rischierebbe di non averla, ci si troverebbe, insomma, dinanzi a un controsenso di fondo: rimettere alla maggioranza (cinque partiti politici su otto) la tutela delle minoranze. Qualora la maggioranza non gradisca l'organizzazione del discorso pubblico prospettata dall'Autorità può disporne sia per sé stessa che anche per le altre forze politiche coinvolte nella competizione elettorale.

È interessante in ultimo fare un cenno, rinviando all'ampia riflessione scientifica sul punto, al fatto che l'AGCOM abbia espressamente posto alla base del proprio parere "la disciplina sulla *par condicio*", che ha ricavato dal «combinato delle disposizioni della

news, Milano, 2017; C.R. Sunstein, #Republic. *La democrazia nell'epoca dei social media*, Bologna, 2017.

[67] Oltre il 90 percento della popolazione fa uso della televisione come mezzo di informazione (AGCOM, *Rapporto sul consumo di informazione*, in *AGCOM.it*, 2018. *Internet*, secondo il medesimo studio, è utilizzato dal 60 percento della popolazione (piazzandosi al secondo posto dopo la televisione con riguardo ai mezzi informativi utilizzati dagli italiani). Su base giornaliera, la differenza è ancora più marcata: oltre il 90 percento degli italiani fa utilizzo del mezzo televisivo, mentre internet si assesta attorno al 42 percento. Riguardo invece all'informazione specificamente politica, il 50,5 percento della popolazione utilizza il mezzo televisivo, mentre internet viene usato dal 34 percento (il 28 percento, in particolare, si affida a fonti algoritmiche, come motori di ricerca e *social network*).

[68] V. *supra*, par. 4.1.

delibera 90/24/CONS e di quelle del provvedimento del 9 aprile 2024 della Commissione parlamentare per l'indirizzo generale e la vigilanza dei servizi radiotelevisivi»[69]. Viene insomma riconfermata la centralità degli strumenti di *soft law* nella disciplina del settore, senza richiamare la fonte primaria in materia[70].

4. Qualche spunto di riflessione

Dalla precedente breve ricostruzione sulla disciplina della *par condicio*, nonché dal caso appena richiamato, possono trarsi alcuni spunti di riflessione, quantomeno sotto due profili: uno relativo alle possibili applicazioni della *par condicio* nel futuro – ma anche nel presente –, segnato dal sempre più diffuso utilizzo di nuove tecnologie, e dunque di nuovi mezzi di comunicazione *(i)*; un altro riguardante il legame tra disciplina della *par condicio* e sistema elettorale, che porta cioè a chiedersi se sia ipotizzabile prevedere una legislazione in tema di comunicazione politica in termini generali, o se questa debba adattarsi al sistema elettorale (e ancor prima dalla forma di governo) in vigore *(ii)*.

4.1. Quale futuro per la *par condicio*?

Con riferimento al primo profilo, posto che una disciplina in tema di parità di trattamento, in quanto "imperativo costituzionale", sia necessaria, ciò non vuol dire che questa non debba essere aggiornata ai tempi e ai mezzi di comunicazione di volta in volta utilizzati per comunicare messaggi (anche) di carattere politico[71]. In altri termini, la disciplina dettata dalla l. 28/2000, va' posta in un contesto evolutivo. È noto – anche l'AGCOM lo ha fatto notare[72] – che grazie alla comunicazione *online*, che si sviluppa

[69] AGCOM, *Comunicato stampa. Chiarimenti sui confronti in tv*, 15 maggio 2024.

[70] Sono stati fatti notare in dottrina i rischi scaturenti da un ricorso smodato ad atti di *soft law* nella regolamentazione di intere materie (cfr., in tal senso, A. Poggi, *Soft Law nell'ordinamento comunitario.* Relazione tenuta al convegno annuale dell'Associazione italiana dei costituzionalisti, Catania, 14-15 ottobre 2005; A. Algostino, *La soft law comunitaria e il diritto statale: conflitto fra ordinamenti o fine del conflitto democratico?*, in *Costituzionalismo.it*, vol. 1, 2017; vi è altresì chi ne difende l'utilità, cfr. D. Morana, *La "legislazione di contorno" del voto referendario in Italia: la disciplina della comunicazione*, in C. De Martin, A. Szmyt-P. Gambale-M. Serowaniec (a cura di), *La democrazia diretta in Italia, Polonia e Unione europea*, Roma, 2020, 321.

[71] La Corte, (Corte cost. 21 aprile 2000, n. 115), individua due criteri, da rispettare contestualmente, con riferimento ai programmi di informazione: i programmi di informazione non possono essere limitati sulla base di motivazioni connesse alla comunicazione politica; le eventuali limitazioni poste ai programmi di informazione – apponibili ai soggetti privati solo nel corso del cd. "periodo elettorale", ex art. 5 c. 1 l. 28/2000 – devono essere volte a prevenire influenze anche surrettizie sulle libere scelte degli elettori; per il resto, viene garantita una massima estensione alla libertà di manifestazione del pensiero in capo ai programmi informativi delle emittenti private. L'Autorità, come fa notare R. Borrello-A. Frosini, *La disciplina delle trasmissioni radiotelevisive di rilievo politico in Italia*, vol. 1, Rimini, 2019, 141 ss., considera unitariamente l'attività radiotelevisiva come di servizio pubblico (a partire dalla l. 223/1990, cd. "legge Mammì"), valorizzando altresì poco la differenza tra informazione e comunicazione politica (R. Borrello, *La par condicio nella campagna elettorale*, cit., 6).

[72] AGCOM, *Segnalazione al governo ai sensi dell'articolo 1, comma 6, lettera c), n. 1 della legge 31 luglio 1997, n. 249 per la revisione della normativa in materia di comunicazione politica e accesso ai mezzi di informazione*, 28 luglio

pressoché in tempo reale, gli esponenti politici sono in costante contatto con gli elettori, i quali possono interagire con essi, commentando e condividendo i contenuti. Essendo l'attuale legge sulla parità di accesso ai mezzi di informazione sorta in risposta a uno specifico contesto politico e sociale in cui versava il Paese sul finire degli anni' 90, e occupandosi dunque quasi esclusivamente del mezzo radiotelevisivo[73], è evidente la necessità di un "ammodernamento" del quadro normativo[74].

Si è fatto notare in dottrina che in questi venticinque anni la legge sulla *par condicio* ha avuto esiti altalenanti, senza riuscire a realizzare ciò che il legislatore si era prefissato[75]. Al contempo, si ritiene tuttavia che i principi che stanno alla base della disciplina siano ancora attuali. Per dirla facendo riferimento alle disposizioni costituzionali, è come se si sostenesse che un sacrificio dell'art. 21 Cost. per tutelare i diritti politici di cui all'art. 48. Cost. sia tuttora necessario, seppur di non semplice attuazione[76]. Un tale bilanciamento, tuttavia, deve essere realizzato con la massima cautela[77], arrecando cioè il minor *vulnus* possibile al lato attivo della libertà di manifestazione del pensiero[78], nonché all'autonomia editoriale.

Se da un lato una disciplina che riguardi unicamente il settore radiotelevisivo è "aggirabile" ricorrendo ai mezzi di comunicazione in rete, dall'altro regolare lo spazio del *web* risulta tutt'altro che agevole, e solleva molteplici problematiche[79]. La questione, quantomeno secondo l'impostazione che altri Paesi europei stanno seguendo, è quella di scegliere tra l'estensione dell'attuale disciplina alle nuove forme di comunicazione

2023.

73 G.E. Vigevani-M. Cazzaniga, *Comunicazione politica e Costituzione*, cit., 16-17. Si tratta della modifica della l. 313/2003 per quanto riguarda la televisione locale, e dell'art. 7 della stessa l. 28/2000 con riferimento alla stampa. Gli Autori fanno anche notare che il confine tra i vari mezzi di informazione si è in realtà assottigliato, essendosi alcuni mezzi di informazione digitale indirizzati più verso un modello che richiama quello televisivo (con "canali di diffusione" e piattaforme video *on demand*), e viceversa l'informazione televisiva fa sempre più utilizzo di interazioni via *social* con i telespettatori.

74 Posizione sostenuta in dottrina, tra gli altri, da G. Gardini, *Brevi note sul divieto di comunicazione istituzionale nei periodi di campagna elettorale*, in questa *Rivista,* 3, 2018, 430.

75 Si rinvia per tutti a R. Borrello, *La par condicio nella campagna elettorale*, cit.

76 Un tale prospettiva sarebbe giustificabile sia riferendosi alla tutela del diritto ad essere informati (A. Papa, *Democrazia della comunicazione e formazione dell'opinione pubblica*, in *federalismi.it*, 1, 2017), o a "non essere disinformati" (cfr. A. Nicita, *Il mercato delle verità*, cit.,), che ragionando in termini di beni costituzionali coinvolti nel bilanciamento (impostazione seguita, tra gli altri, da A. Pace, *Libertà di informare e diritto ad essere informati. Due prospettive a confronto nell'interpretazione e nelle prime applicazioni dell'art. 7, co.1, del T.U. della radiotelevisione*, in *Diritto pubblico*, 2, 2007, 459 ss.

77 La libertà di manifestazione del pensiero è, secondo autorevole dottrina, quella che più di tutte concorre alla forma di Stato (R. Zaccaria, A. Valastro-E. Albanesi, *Diritto dell'informazione e della comunicazione*, cit., 2).

78 Secondo l'impostazione di C.R. Sunstein, *Liars. Falsehoods and free speech in age of deception*, Oxford, 2021.

79 Come detto, il tema della regolamentazione dell'informazione su internet è sommamente complicato, e riguarda in modo particolare i soggetti "mediatori" delle informazione, tanto che tale regolamentazione è stata assimilata a un triangolo da J. Balkin, *Free speech is a triangle*, in *Columbia Law Review*, 7:118, 2011, 2018 ss.; La previsione di una responsabilità in capo alle piatteforme solleverebbe, tra gli altri, il non trascurabile problema della *collateral censorship* (J. Balkin, *Free speech and hostile environments*, in *Columbia Law Review*, 8:99, 1999).

(strutturalmente diverse) o il ricorso alla creazione di una nuova disciplina *ad hoc*[80].
Tornando agli esiti poco soddisfacenti raggiunti dalla l. 28/2000, emerge un elemento chiaro: il punto su cui si gioca la parità di trattamento non è l'uguale spazio in termini di tempo[81], quanto «il potere di dettare l'agenda e di definire i temi del dibattito pubblico»[82] in capo ai soggetti coinvolti nella competizione elettorale. Si è così "scaricato un peso" – sulla normativa positiva – che la sola disciplina legislativa[83] non è in grado di supportare, specie facendo riferimento a – pur sofisticati e per certi versi necessari – criteri "matematici" (si pensi, ad esempio, al problema del pluralismo interno in Rai, cui in questa sede si fa solo rinvio[84]).
Sono dunque necessarie nuove regole, o comunque strumenti nuovi per la regolazione dell'ecosistema digitale? Si conviene con quanto sostenuto da parte della dottrina, secondo cui le soluzioni dovranno probabilmente essere diversificate e multidisciplinari, ma che debbano al contempo fare riferimento alla "cassetta degli attrezzi" propria di quello che è stato definito il costituzionalismo «senza aggettivi»[85], ovvero ricorrendo agli strumenti già previsti nell'alveo della tradizione del diritto costituzionale liberaldemocratico. In tal senso, alcune regole già previste dalla disciplina attualmente in vigore paiono estendibili ai *social media* (quali il silenzio elettorale, il divieto di pubblicazione di sondaggi nel periodo antecedente alla consultazione elettorale, la disciplina sulla comunicazione istituzionale ex art. 9 l. 28/2002), altre sembrano invece incompatibili (è difficile ragionare in termini di "parità" riguardo alle pubblicazioni, di diversissime tipologie, sui *social network*). Il nodo centrale in questo senso pare essere quello legato alla trasparenza, in tema di messaggi elettorali (prevedendo obblighi in capo alle piattaforme circa l'indicazione dei profili da cui provengono le pubblicazioni) e di definizione delle procedure che permettono la segnalazione all'autorità dei contenuti che violino le disposizioni sulla parità di trattamento. È la direzione che l'AGCOM ha iniziato ad assumere nel 2020 con riferimento ai messaggi politico-elettorali, per cui

[80] R. Borrello, *La par condicio nella campagna elettorale*, cit., 25.

[81] Sull'applicazione "matematica" e quantitativa della disciplina sulla *par condicio*, cfr. R. Borrello, *La par condicio nella campagna elettorale*, cit., 4; O. Grandinetti, *La par condicio al tempo dei social*, cit., 101. Un interrogativo collaterale è quello relativo alla funzionalizzazione sia della televisione pubblica che di quella privata ex art. 7 Tusmar. La Corte costituzionale (Corte cost. 24 aprile 2002, n. 155) ha sancito il principio della tutela «dell'identità politica delle singole emittenti private», che hanno la possibilità di far emergere una propria immagine tramite considerazioni di ordine politico. Secondo la "sentenza decalogo" della Corte di Cassazione (Cass. civ., sez. I, 18 ottobre 1984, n. 5259, in *Nuova Giurisprudenza Civile Commentata*, 1, 1985), i mezzi privati sarebbero vincolati solo nel periodo elettorale (seppur potrebbero già, per quanto detto, avere una propria legittima connotazione).

[82] G.E. Vigevani-M. Cazzaniga, *Comunicazione politica e Costituzione*, cit., 29.

[83] O. Grandinetti, *La par condicio al tempo dei social*, cit., 96.

[84] G.E. Vigevani, *Fondamento costituzionale e autonomia nei media di servizio pubblico nell'era della rete*, Torino, 2017, 229 ss.; O. Grandinetti, *La governance della Rai e la riforma del 2015*, in *Rivista trimestrale di diritto pubblico*, 3, 2016, 833 ss.; in chiave europea, E. Brogi, *Media pluralism monitor 2016 – Monitoring risks for media pluralism in the EU and beyond – Country report: Italy (indagine del CMPF, Centre for Media pluralism and media freedom),* Roma, 2017; riguardo al pluralismo esterno, come riportato da AGCOM*, Relazione annuale 2018*, cit., 119 ss. i dati sono i seguenti: Rai 42,4% – 46,2% dell'audience share, Mediaset 27,7% - 37%, Skytg24 0,59%, per cui si assiste di fatto ancora a un duopolio in campo televisivo.

[85] M. Luciani, *Relazione conclusiva. Convegno "Il diritto costituzionale e le sfide dell'innovazione tecnologica"*, in *Rivista del Gruppo di Pisa*, 3, 2021; M. Betzu, *I baroni del digitale*, Napoli, 2022; F. Paruzzo, *I sovrani della rete*, Torino, 2022.

alle piattaforme digitali viene richiesto, prima che il contenuto venga pubblicato, di eseguire un controllo sull'account che intende pubblicare il contenuto stesso, così da accertarsi che non si tratti di un *bot* o di un "*account fake*"[86].
In sintesi, si conviene pertanto con chi sostiene che sia necessario un approccio multidisciplinare[87], che tenga cioè insieme la disciplina del settore dell'informazione e le regolamentazioni in ambito di trasparenza e *privacy*.
Resta il fatto che sarebbe illusorio scaricare l'intero onere del buon funzionamento del sistema dell'informazione e della comunicazione politica su previsioni normative; fino a quando «non si raggiungerà uno standard accettabile per quanto concerne la garanzia del pluralismo e dell'indipendenza dei *media* rispetto al potere politico ed economico, qualsiasi normativa in questi settori rimarrà solamente un succedaneo se non addirittura un placebo»[88]. Tenendo presente che quando si tratta di *par condicio* sul *web*, l'indipendenza è da garantire principalmente rispetto a poteri privati, che svolgono il ruolo di *gatekeepers* dell'informazione, anche in ambito politico-elettorale[89].

4.2. Il legame tra *par condicio* e sistema elettorale

La normativa italiana sulla *par condicio* ricalca, come detto[90], il modello francese, pensato per una forma di governo – e un sistema elettorale – profondamente diversi. Quando la legge sulla *par condicio* fu approvata era in vigore una legge elettorale di tipo maggioritario[91], che portò alla (temporanea) affermazione di un tendenziale bipolarismo nel Paese, e che ha segnato in qualche modo sia l'impostazione della normativa, che le modalità in cui si articola il dibattito pubblico e il confronto tra le diverse forze politiche. Il legislatore si è mostrato consapevole della questione, tanto da prevedere all'art. 4 c. 2 lett. *b)* l. 28/2002 un riferimento al sistema elettorale quale parametro che l'Autorità e la Commissione di vigilanza devono valutare per la ripartizione degli spazi tra i soggetti politici. È stato tuttavia fatto notare che la legge nella sua impostazione generale risente del sistema elettorale e del contesto sociopolitico del tempo[92]; l'idea trasversale che culturalmente segnava – e forse segna tuttora – il dibattito pubblico è quella per cui le elezioni vanno "vinte", i "vincitori" devono governare, il Governo

[86] AGCOM, *Impegni assunti dalle società esercenti le piattaforme on line per garantire la parità di accesso dei soggetti politici alle piattaforme digitali durante le campagne per il referendum popolare confermativo relativo al testo della legge costituzionale recante "Modifiche degli articoli 56, 57 e 59 della Costituzione in materia di riduzione del numero dei parlamentari", e per le elezioni del Presidente della Giunta Regionale e del Consiglio Regionale delle Regioni Liguria, Veneto, Toscana, Marche, Campania, Puglia e Valle d'Aosta, indette per i giorni 20 e 21 settembre 2020*, 5 agosto 2020.

[87] O. Grandinetti, *La par condicio al tempo dei social*, cit., 125.

[88] G.E. Vigevani-M. Cazzaniga, *Comunicazione politica e Costituzione*, cit., 29.

[89] G. Pitruzzella, *La libertà di informazione nell'era di internet*, in G. Pitruzzella-O. Pollicino-S. Quintarelli (a cura di), *Parole e potere*, cit.

[90] Se ne è fatto cenno *supra*, par. 3.

[91] L. 276/1993 (cd. "*Mattarellum*").

[92] Cfr. G. Sirianni, *Par condicio: i complessi rapporti tra potere politico e potere televisivo*, in *Politica del diritto*, 4, 2005, 625 ss.

deve essere "scelto" dagli elettori e così via. Posto che una visione del genere mal si concilia con la forma di governo parlamentare[93], va da sé che quelle del Parlamento europeo sono elezioni che non "si vincono" (ovvero non vi è una parte che prevale sull'altra e assume compiti di governo), ma in cui si fotografa l'esistente[94]. Insomma, a maggior ragione nell'ambito di una competizione elettorale basata su un sistema proporzionale non pare facilmente applicabile né il *format* dei "duelli" televisivi (si veda in tal senso il richiamato caso del confronto Meloni-Schlein[95]), né in generale il criterio matematico del conteggio delle presenze – già contestabile, come visto, di per sé –, in quanto il cuore della disciplina consiste nell'evitare che su determinati temi alcune forze politiche possano essere irragionevolmente escluse dal dibattito pubblico, ovvero che alcune possano dettare l'agenda pubblica più di altre. Per certi versi, dunque, potrebbe sostenersi che la concezione e le forme di organizzazione della politica – e dunque delle elezioni – che caratterizzano un sistema proporzionale non sono facilmente conciliabili con i "confronti a due". Un sistema proporzionale non riflette, per utilizzare le categorie di G. Sartori, una concezione della «democrazia come guerra», ma è improntato alla «democrazia come trattativa» [96]. In altri termini, un sistema elettorale proporzionale non mira a creare – anche artificialmente se necessario – una maggioranza o un "vincitore"[97], bensì tende a fotografare e riprodurre il complesso e frastagliato panorama politico, in modo che la decisione sorga come compromesso tra visioni politiche – e anche ideologiche – contrapposte[98]. Si badi bene: "democrazia come trattativa" equivale a "democrazia senza conflitto". Anzi, forse significa proprio il contrario: «c'è bisogno di un conflitto permanente perché si possa trattare. È, al contrario, la democrazia come guerra che, mirando a sancire un vincitore, annulla il conflitto politico, sterilizzandolo sino alle elezioni successive»[99]. Il conflitto, in una "democrazia come trattativa", è un costante tentativo di rispondere in modo politicamente maturo alle molteplici conflittualità che segnano il vivere sociale. Come si apprende dall'insegnamento kelseniano[100], il conflitto non va addomesticato, negato o contenuto, ma è l'unica fonte di progresso sociale. La logica sottostante a un sistema proporzionale mostra dunque come sia altresì illusorio applicare una disciplina soltanto «per il tempo intercorrente tra la data di presentazione delle candidature e la data di chiusura della campagna»[101] Il rischio è pertanto quello di "verticizzare" il

93 F. Pallante, *Introduzione*, in F. Pallante (a cura di), *Difesa della proporzionale. Il dibattito ne "La Rivoluzione Liberale", 1922-1925, di Piero Gobetti e i suoi collaboratori*, Fano, 2024.

94 Si rinvia a Corte cost., 15 gennaio 2013, n. 1.

95 V. *supra*, par. III.

96 G. Sartori, *Tecniche decisionali e sistema dei comitati*, in *Rivista italiana di scienza politica*, 1, 1974.

97 O a garantire governabilità, cfr. G. Zagrebelsky-V. Marcenò-F. Pallante, *Lineamenti di diritto costituzionale*, cit., 326.

98 F. Pallante, *Introduzione*, in P. Gobetti, *Difesa della proporzionale*, cit., 8.-9; Si v. anche il già citato G. Sartori, *Tecniche decisionali e sistema dei comitati*, cit., 22 ss., secondo cui la democrazia come guerra è "un gioco a somma nulla", mentre la democrazia come trattativa è un gioco a "somma positiva", come dimostrerebbe, nel caso italiano, la stagione di riforma degli anni '70.

99 F. Pallante, *Introduzione*, cit., 11.

100 H. Kelsen, *Democrazia*, Bologna, 2010.

101 Art. 4 c. 2 l. 28/2000, che cita i sistemi elettorali quale fattore su cui "tarare" l'informazione politica

conflitto e ridurlo al solo momento elettorale, di fatto anestetizzandolo e rendendolo sterile. Da ciò si evince che il sistema elettorale adottato, influenzando l'organizzazione delle forze politiche coinvolte nel momento elettorale, influisce altresì sull'assetto del discorso pubblico: in caso di elezioni di un organo esecutivo, o di sistema elettorale maggioritario segnato da un bipolarismo politico, il *format* del "duello" può essere più facilmente (e auspicabilmente) applicato, così come il criterio matematico delle presenze nelle trasmissioni televisive risulta meno deformante; quando viene eletto un organo legislativo con sistema proporzionale la previsioni di confronti a due diventa invece più problematiche, richiedendo un lavoro non agevole sui sistemi di compensazione[102], e rendendo in ogni caso insoddisfacente e fittizio il criterio di conteggio quantitativo delle presenze.

Fa sfondo alle riflessioni in materia il fatto che i media tradizionali, pur essendo nel caso della televisione ancora quelli maggiormente diffusi, influiscono sempre meno sulla formazione delle opinioni politiche dei cittadini, che li considerano sempre di più inutili o comunque parziali, ovvero mediati in maniera precostituita dall'editore o giornalista di turno[103]. Diversi studi settoriali sul punto mostrano come a volte proprio perché non mediata, o perché mediata in maniera apertamente faziosa da *youtuber* o *influencer*, l'informazione non giornalistica o televisiva viene percepita dagli elettori come più trasparente, credibile e diretta. Ciò mostra come sia illusorio pensare che una riforma normativa possa da sola risolvere un problema ampio, che, oltre ai punti già evidenziati[104], interessa un profondo problema culturale che interessa sia le classi politiche che l'elettorato, ovvero i destinatari della comunicazione politica[105].

Tirando le fila del discorso emerge che le soluzioni "estreme" o monodirezionali (rendere ancora più rigida e pervasiva la logica della parità di trattamento a livello cronologico da un lato, o lasciare campo libero alle forze politiche, editoriali ed economiche di organizzare i prodotti di informazione e comunicazione politica dall'altro) in tema di *par condicio* lasciano insoddisfatti. La disciplina sulla *par condicio* necessita di un ammodernamento, pur non potendosi allargare acriticamente ai *social network* l'intero complesso normativo in vigore. Ciò richiede un approccio di tipo multidisciplinare, con partico-

in tempo di campagna elettorale.

[102] L'AGCOM, nel caso in esame, ci ha provato, mostrando che è su nuovi format giornalistici che probabilmente bisogna riflettere.

[103] Quantomeno nel contesto americano, con riferimento alle elezioni presidenziali del 2024, il *trend* tuttavia sta già cambiando: «Anche i grandi network televisivi, con i loro canali *all news*, hanno mostrato segni di una perdita progressiva e consistente di rilevanza, anche nella fase delle campagne elettorali e delle elezioni, storicamente il momento in cui attirano le maggiori attenzioni e i più consistenti investimenti pubblicitari. Continuano ad avere grandi *audience* nei momenti più importanti della campagna, come i confronti televisivi fra i candidati, ma in generale il loro pubblico è in calo. L'*audience* complessiva dei tre maggiori (nell'ordine Fox News, MSNBC e CNN) è diminuita del 32 per cento rispetto al 2020, scendendo intorno ai 21 milioni nel giorno medio, con cali più consistenti per CNN, che ha perso oltre la metà dei suoi spettatori. Per tutte e tre le televisioni si tratta poi di spettatori particolarmente anziani, con un'età mediana fra i 67 e i 70 anni», Il Post, *Il dibattito sul potere dei giornali dopo la vittoria di Trump*, 14 novembre 2024, e I. Simonetti, J. Flint, *TV Networks embrace their aging audience with a new mantra: age doesn't matter*, in *Wall Street Journal*, 22 maggio 2024.

[104] V. *supra*, par. 3.

[105] Occorre una riflessione anche sulla domanda dell'informazione, come sostenuto da V. Visco Comandini, *Le fake news sui social network*, cit.

lare attenzione al tema della trasparenza, che però potrebbe non essere sufficiente se non "sostenuto" da altri interventi normativi congiunti in tema di pluralismo interno ed esterno, nonché da fattori politici, culturali e sociali, tenendo presente che anche il sistema elettorale adottato influenza la conformità alla disciplina normativa dei *format* di informazione e comunicazione politica che i mezzi di informazione propongono.

Se gli *e-Sports* non sono (soltanto) un gioco. Qualche riflessione sull'inquadramento giuslavoristico del *pro-player**

Marianna Russo

Abstract

Qual è l'inquadramento giuslavoristico del *pro-player*? Quali sono le tutele previste per l'attività e-sportiva? Il contributo intende rispondere a questi rilevanti interrogativi esaminando il fenomeno degli *e-Sports* e le loro implicazioni giuslavoristiche, in vista di una futura regolamentazione.

What is the labour law framework for the pro-player? What are the protections provided for e-Sports activities? This paper aims to answer these important questions by examining the phenomenon of e-Sports and their labour law implications, with a view to future regulation.

Sommario

Keywords

e-Sports – pro-player – lavoro digitale – rischi psicofisici – protezione

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

1. Note introduttive sul lavoro digitale

Anche se è ormai in atto da decenni[1], la tecnologizzazione del lavoro continua a sorprendere e pungolare l'interprete, aprendo quotidianamente scenari inesplorati e sollecitando soluzioni giuridiche tempestive, perché la rivoluzione tecnologica sfida i «vecchi diritti», ma, al contempo, ne esige «impetuosamente di nuovi»[2].

La stessa definizione di lavoro tecnologico o – più correttamente – digitale risulta piuttosto controversa. Comunemente, gli aggettivi "tecnologico" e "digitale" vengono adoperati in maniera fungibile, come sinonimi[3]. In realtà, si tratta di nozioni distinte, che potrebbero avere tra di loro il rapporto da *genus* a *species*. La tecnologia[4] rappresenta quell'ambito di «ricerca multidisciplinare con oggetto lo sviluppo e l'applicazione di strumenti tecnici, ossia di quanto è applicabile alla soluzione di problemi pratici, all'ottimizzazione di procedure, alla presa di decisioni, alla scelta di strategie finalizzate a dati obiettivi, sulla base di conoscenze scientifiche, comprese quelle matematiche e informatiche»[5]. Intesa in senso ampio, la tecnologia abbraccia sia il sistema analogico – adoperato fin dalla seconda metà del diciannovesimo secolo e basato sulla manipolazione di segnali o informazioni rappresentati in forma continua – sia quello digitale[6], che trasmette i dati in forma binaria (i c.d. bit). La vera rivoluzione tecnologica del ventunesimo secolo è costituita proprio dall'avvento della digitalizzazione: dal 2002 l'immagazzinamento di informazioni in forma digitale ha soppiantato quello in modalità analogica. La digitalizzazione è, così, diventata la nuova frontiera dello sviluppo tecnologico, penetrando in tutti gli ambiti della quotidianità, organizzazione del lavoro compresa. Considerato che l'attuale connessione ad Internet si avvale esclusivamente di segnali di tipo digitale, le prestazioni lavorative svolte mediante dispositivi elettronici connessi alla rete possono essere correttamente considerate "digitali".

I dubbi interpretativi, però, non riguardano soltanto il significato e l'etimologia dei termini in uso, ma, soprattutto, l'individuazione di cosa sia il lavoro digitale[7] o, meglio, di chi possa essere considerato lavoratore digitale. A livello internazionale ed europeo, punto di riferimento imprescindibile per l'analisi dell'impatto delle nuove tecnologie nel mondo del lavoro è il report Eurofound-ILO *Working anytime anywhere: the effects on the world of work*[8]. Il campo d'indagine, però, risulta piuttosto circoscritto, in quanto

---

[1] Cfr. G. Vardaro, *Tecnica, tecnologia e ideologia della tecnica nel diritto del lavoro*, in *Politica del diritto*, 1, 1986, 75 ss.; S. Simitis, *Juridification of labor relations*, in G. Teubner (a cura di), *Juridification of social spheres: a comparative analysis in the areas of labor, corporate, antitrust and social welfare law*, Firenze, 1987, 150 ss.

[2] S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, 15.

[3] Anche il Parlamento Europeo, nella risoluzione del 21 gennaio 2021 con raccomandazioni alla Commissione sul diritto alla disconnessione, utilizza indistintamente i due termini: v. ad es., nel preambolo, la lett. A («*digital tools*») e la lett. E («*technological devices*»).

[4] Dal greco τέχνη, tecnica, e λογία, discorso.

[5] Enc. Treccani online.

[6] Dall'inglese *digit* (che deriva dal latino *digitus*, dito), che significa numero, cifra.

[7] L'aggettivo "digitale" risulta, in questo caso, più specifico, ma nulla vieta che si possa parlare di lavoro tecnologico in senso ampio.

[8] Eurofound-ILO, *Working anytime anywhere: the effects on the world of work*, Ginevra, 2017, 6.

prende in considerazione soltanto i lavoratori dipendenti[9] che adoperano le tecnologie T/ICTM – ossia i sistemi integrati di telecomunicazione per creare, immagazzinare e scambiare informazioni – purché la prestazione sia svolta, almeno occasionalmente, al di fuori dei locali aziendali[10]. Questa lettura – che risale al 2017, ossia prima dell'accelerazione impressa alla digitalizzazione del lavoro dalla pandemia da Covid-19 – potrebbe ritenersi ormai superata, in quanto i confini del lavoro digitale si presentano molto più ampi, superando sia ogni distinzione di qualificazione giuridica del rapporto, sia il riferimento al luogo di svolgimento della prestazione. Da un lato, non si può dubitare che rientrino a pieno titolo nel novero dei lavoratori digitali i c.d. *platform workers*[11], pur trattandosi generalmente di lavoratori autonomi[12]. D'altro canto, non è ravvisabile alcuna ragione ostativa nell'inclusione dei lavoratori subordinati che adoperino (esclusivamente o, comunque, prevalentemente) dispositivi elettronici per lo svolgimento della prestazione lavorativa, anche nell'ambito del tradizionale luogo di lavoro[13].

Il lavoro digitale può abbracciare qualsiasi prestazione lavorativa resa attraverso l'ausilio di strumentazioni elettroniche connesse alla rete, come si deduce dal considerando n. 11 della proposta di direttiva UE allegata alla risoluzione in materia di disconnessione[14]: «il diritto alla disconnessione dovrebbe applicarsi a tutti i lavoratori e a tutti i settori, sia pubblici che privati», in quanto l'utilizzo delle tecnologie digitali investe tutte le tipologie di lavoratori, trasformando i modelli tradizionali di lavoro.

Un altro aspetto da considerare per individuare correttamente il lavoro digitale è la non mera occasionalità nell'utilizzo dei dispositivi digitali. Tali strumenti devono essere parte integrante della prestazione lavorativa, in maniera esclusiva o prevalente[15].

---

[9] L'adozione, nel Report, del termine "*employees*" circoscrive l'indagine ai lavoratori subordinati.

[10] *Home-based teleworkers*, cioè telelavoratori, e *high mobile T/ICTM employees* oppure *occasional T/ICTM employees*, che, per la normativa italiana, corrisponderebbero ai lavoratori agili.

[11] Secondo la ricerca condotta dal Consiglio dell'Unione Europea, in Europa operano circa 28.000.000 di lavoratori delle piattaforme digitali, di cui il 93% risulta qualificato come lavoratore autonomo.

[12] Al riguardo, v. la direttiva (UE) 2024/2831 del 23 ottobre 2024, secondo la quale «attualmente si stima che nove piattaforme su 10 tra quelle attive nell'UE classifichino le persone che vi lavorano come lavoratori autonomi». Sul dibattito qualificatorio innescato in Italia dall'art. 47 *bis* d. lgs. 81/2015, v., *ex multis*, U. Carabelli, *Brevi note sulla nuova disciplina del lavoro non subordinato tramite piattaforma anche digitale,* in *Bollettino ADAPT*, 10, 2019; E. Raimondi, *Il lavoro nelle piattaforme digitali e il problema della qualificazione della fattispecie*, in *Labour & Law Issues*, 2, 2019, 85; F. Carinci, *L'art. 2 d.lgs. n. 81/2015 ad un primo vaglio della Suprema Corte: Cass. 24 gennaio 2020, n. 1663*, in *CSDLE Biblioteca 20 Maggio,* 1, 2020, 161 s.; A. Perulli, *Il diritto del lavoro "oltre la subordinazione": le collaborazioni etero-organizzate e le tutele minime per i riders autonomi*, in *CSLDE "Massimo D'Antona"*, 410, 2020; O. Razzolini, *I confini tra subordinazione, collaborazioni etero-organizzate e lavoro autonomo coordinato: una rilettura*, in *Diritto delle Relazioni Industriali*, 2, 2020, 1 ss.; C. Spinelli, *Le nuove tutele dei riders al vaglio della giurisprudenza: prime indicazioni applicative*, in *Labour & Law Issues*, 1, 2020, 89; A. Perulli*, Il rider di Glovo: tra subordinazione, etero-organizzazione, e libertà*, in *Argomenti di Diritto del Lavoro*, 1, 2021, 37.

[13] I dipendenti «*always at the employer's premises with ICT*» secondo la classificazione riportata nel report Eurofound-ILO, *Working anytime*, cit., 7.

[14] Risoluzione del Parlamento europeo del 21.1.2021.

[15] Nella visione accolta dal presente contributo, rientra sicuramente nell'ambito del lavoro digitale l'attività dell'operaio che, per lo svolgimento della propria prestazione, sia tenuto a indossare la c.d. *wearable technology*. Al contrario, l'operaio che, nell'esecuzione delle sue mansioni, adoperi soltanto strumenti meccanici, ma utilizzi in via eccezionale lo *smartphone* personale per avvisare il capo squadra del verificarsi di un pericolo, non potrebbe essere definito lavoratore digitale. In quest'ultima ipotesi, l'uso di un dispositivo digitale – peraltro personale – è soltanto sporadico ed eventuale.

L'individuazione del perimetro del lavoro digitale – che ormai riguarda larga parte dei lavoratori[16] – è essenziale. La disciplina di tali rapporti richiede particolare attenzione sia nel contemperamento tra l'organizzazione del lavoro digitale – finalizzata a rendere la prestazione più rapida, efficiente e conveniente – e la garanzia dei diritti fondamentali dei lavoratori (alla riservatezza, al rispetto dei tempi di riposo, all'effettivo esercizio dell'attività sindacale…), sia nella predisposizione di tutele adeguate avverso gli insidiosi rischi fisici e psicosociali collegati alla digitalizzazione.

2. L'evoluzione degli *e-Sports*

Nell'ampio e variegato panorama dei lavori digitali, particolare attenzione meritano coloro che svolgono prestazioni a vario titolo nell'ambito dei c.d. *e-Sports*, ossia delle competizioni e attività sportive effettuate, in via professionale, mediante videogiochi[17]. È un fenomeno che, ormai da decenni, coinvolge un considerevole numero di soggetti e molteplici figure professionali, nonché un significativo volume d'affari.
La prima competizione sportiva basata su un videogioco[18], sponsorizzata dalla rivista *Rolling Stone*[19], è stata organizzata nel 1972 dall'Università di Stanford, in California, con una ventina di partecipanti. Nel corso degli anni l'interesse nei confronti dei tornei di *videogames*[20] è aumentato in maniera esponenziale, come attesta il primo campionato internazionale professionistico[21], tenutosi nel 1997 con circa duemila partecipanti, dapprima virtualmente e poi ad Atlanta, negli Stati Uniti, per la finale[22]. Lo stesso anno sono state fondate la *Cyberathlete Professional League*[23] e la *Professional Gamers League*[24], le prime organizzazioni professionistiche per i *cyber*-atleti[25].
Negli anni 2000 si è assistito ad un'ampia diffusione degli *e-Sports* grazie alla possibilità di utilizzare tecnologie e piattaforme digitali sempre più sofisticate e alla crescente disponibilità di piattaforme multimediali in *streaming online*[26]. Il coinvolgimento di un

[16] V. M. Russo, *Esiste il diritto alla disconnessione? Qualche spunto di riflessione alla ricerca di un equilibrio tra tecnologia, lavoro e vita privata*, in *Diritto delle Relazioni Industriali*, 3, 2020, 682.

[17] J. Ierussi - C. Rombolà, *Esports: cosa sono?,* in *Rivista di Diritto Sportivo*, 2, 2018, 308.

[18] Per la precisione, *Spacewar*, considerato uno dei primi videogiochi in senso moderno. Ideato nel 1961 da Martin Graetz, Stephen Russell e Wayne Wiitanen, è stato realizzato sul processore digitale PDP-1 da Stephen Russell, Peter Samson, Dan Edwards e Martin Graetz, insieme ad Alan Kotok, Steve Piner, e Robert A Saunders: v. *masswerk.at/spacewar/*.

[19] V. *esportsitalia.com/quando-sono-nati-gli-esports-la-storia-del-progaming/*.

[20] I videogiochi, nel corso del tempo, sono diventati sempre più sofisticati. Tra i più utilizzati nelle competizioni sportive professionistiche possono essere annoverati *StarCraft*, *Warcraft*, *Fortnite*, FIFA, PES.

[21] Basato sul videogioco *Quake*.

[22] V. *History of Esports*, in Futureparty, 2 febbraio 2022.

[23] V. *cyberathlete.com/cpl/*.

[24] V. *pglesports.com/*.

[25] Per un approfondimento, v. F. Larch, *eSports History*, in *ISPO*, 2 agosto 2023.

[26] Nel 2011 è stata fondata *Twich.tv*, inizialmente incentrata su videogiochi e sport elettronici. Sul punto, v. A. Maietta, *Gli e-sports: stato attuale e prospettive di inquadramento normativo*, in *Rivista di Diritto Sportivo*, 5 ottobre 2022, che mette in evidenza come «il volano dello sviluppo degli e-sport è stato

numero sempre maggiore di giocatori ha attratto anche numerosi sponsor, consentendo un significativo aumento dei montepremi per questo tipo di competizioni, fino a raggiungere cifre da capogiro[27]. L'impatto economico non è per nulla trascurabile: secondo una ricerca condotta da NewZoo e Deloitte, l'industria degli *e-Sport* nel 2015 ha generato un fatturato di circa 400 milioni di dollari[28].

Con l'avvento della pandemia da Covid-19 e i lunghi periodi di *lockdown* che hanno interessato numerosi Paesi a livello mondiale, il mercato degli *e-Sports* ha registrato un'impennata, a cui, però, ha fatto seguito un rallentamento nel corso del 2022, come riporta lo studio di Deloitte, che prende in considerazione 22 nazioni, tra le quali 11 Stati membri dell'Unione Europea[29].

L'Italia – insieme alla Spagna e alla Polonia – risulta uno dei Paesi con il maggiore *engagement* nei confronti del *gaming*, ossia con un elevato coinvolgimento dei fan, soprattutto di età più giovanile. Ciò comporta un considerevole impatto sia a livello sociale che economico. In particolare, gli *e-Sports* attirano investimenti da parte delle imprese interessate a intercettare il *target* della c.d. generazione Z. Eppure, nonostante la diffusione del *gaming* e l'interesse mediatico suscitato[30], il riconoscimento e la promozione del settore degli *e-Sports* in Italia presenta ritardi strutturali e normativi, come rilevato dall'Osservatorio Italiano E-Sports (OIES) nel 2023[31].

3. I tentativi di regolamentazione degli sport elettronici

L'esigenza di disciplinare gli *e-Sports* non è certamente ignorata, né a livello nazionale né sovranazionale. Il 10 novembre 2022 il Parlamento europeo ha emanato una risoluzione sugli sport elettronici che riconosce il valore fondamentale dell'ecosistema videoludico all'interno del panorama economico europeo. Il punto 18 della risoluzione sottolinea come i videogiochi siano parte integrante del patrimonio culturale europeo[32], mentre il punto 19 mette in evidenza la loro finalità didattica ed educativa[33],

sia la diffusione delle connessioni a *internet* veloce a banda larga e ultralarga, sia lo *streaming online*». Inoltre, come sottolinea F. Santini, *Il microcosmo videoludico: gli Esports*, in M. Biasi (a cura di), *Diritto del lavoro e intelligenza artificiale*, Milano, 2024, 691, «la diffusione dell'Intelligenza Artificiale pare destinata a spingere oltre lo sviluppo anche dell'ecosistema videoludico». V. anche C. Di Carluccio, *Non è solo un videogioco! Il lavoro dei pro-players nell'ecosistema degli e-sports*, in *Judicium*, 2 ottobre 2024.

27 Nell'ordine di milioni di dollari.

28 V. *Esport: mercato a 400 milioni di dollari,* in *E-duesse,* 27 gennaio 2016.

29 Deloitte, *Let's Play! 2022 The European esports market*, 28 novembre 2022.

30 Basti pensare che il portale DAZN trasmette in *streaming* i tornei di videogiochi.

31 OIES, *White Paper Esports e gaming in Italia 2023*, in *oiesports.it.*

32 Il 24 novembre 2023 il Consiglio dell'Unione Europea, nell'ambito del Piano di lavoro europeo per la cultura 2023-2026, ha approvato le Conclusioni sul rafforzamento della dimensione culturale e creativa del settore europeo dei videogiochi. In particolare, il Consiglio ha rimarcato come il mondo dei videogiochi non solo interagisca con i settori economici, contribuendo alla crescita del PIL europeo, ma incentivi altresì la trasmissione di contenuti culturali, sviluppando un comparto industriale che, per definizione, è fondato sulla ricerca e sull'innovazione tecnologica.

33 V. punto 35 in riferimento al rilevante contributo degli sport elettronici e dei videogiochi nella sensibilizzazione su questioni climatiche e ambientali.

soprattutto per i fanciulli[34]. Il punto 33 della risoluzione si sofferma sui possibili rischi psicosociali collegati all'utilizzo intensivo dei videogiochi[35].
Anche se sono molteplici le questioni affrontate dalla risoluzione, è opportuno ricordare che si tratta di un provvedimento privo di efficacia vincolante. La risoluzione è, infatti, un atto atipico, in quanto non espressamente incluso nell'elenco degli atti giuridici dell'Unione Europea riportato dall'art. 288 del Trattato sul Funzionamento dell'Unione Europea. Di conseguenza, per quanto rappresenti un prezioso incoraggiamento nella regolazione degli *e-Sports*, il valore effettivo della risoluzione è soltanto simbolico.
A livello nazionale, l'Italia ha manifestato il suo interesse alla regolamentazione del fenomeno, come attestato dalla proposta di legge n. 868 sulla disciplina degli sport elettronici o virtuali e delle connesse attività professionali ed economiche, presentata alla Camera il 7 febbraio 2023, e dal disegno di legge n. 970 sulla regolamentazione delle competizioni videoludiche, attualmente in corso di esame nella settima Commissione del Senato[36]. Nella relazione introduttiva di tali provvedimenti si sottolinea il notevole impatto economico e sociale del settore videoludico[37], nonché «l'effetto domino» realizzato dal nuovo scenario della digitalizzazione attorno al settore dei videogiochi[38], che ormai travalica le mere comunità di amici riunitesi per puro intrattenimento e coinvolge molteplici soggetti, in maniera professionale, a vari livelli (locale, nazionale e internazionale), esigendo, di conseguenza, una disciplina giuridica di riferimento.
I tentativi – europeo e italiano – di regolazione del *gaming* e dei soggetti coinvolti si rivelano molto stimolanti per gli aspetti trattati e, ancor più, per quelli non affrontati espressamente. Sono proprio i coni d'ombra sulla materia a lasciar trasparire le maggiori criticità.

4. Le principali criticità: l'individuazione del *pro-player*

Nella prospettiva giuslavoristica le criticità sottese alla regolamentazione degli sport

[34] Il Commento generale n. 25 del 2021 sui diritti del fanciullo nell'ambiente digitale, adottato dal Comitato delle Nazioni Unite sui Diritti dell'Infanzia, afferma che le tecnologie digitali sono "vitali" per la vita ed il futuro dei bambini e degli adolescenti. Per un approfondimento, v. G. Bevilacqua, *Verso il metaverso dei giochi: tra diritti del fanciullo e azioni responsabili dell'industria del gaming*, in A. Fuccillo - V. Nuzzo - M. Rubino De Ritis (a cura di), *Diritto e universi paralleli. I diritti costituzionali nel metaverso*, Napoli, 2023, 373.

[35] Mentre l'abnegazione nei confronti di uno sport tradizionale viene sempre considerata positiva, l'eccesso di *gaming* desta preoccupazione. Già nel 2018 l'Organizzazione Mondiale della Sanità ha inserito l'esercizio smodato del gaming nell'undicesima revisione della classificazione internazionale delle malattie mondiali come "*addictive gaming disorder*".

[36] Al 12 dicembre 2024, l'ultimo aggiornamento riportato dal sito-*web* del Senato è l'esame del disegno di legge in Commissione alla data del 10 aprile 2024. Anche nella precedente legislatura sono state presentate due proposte di legge, la n. 3626 e la n. 3679, che hanno tentato di «ricondurre ad unità l'ampio spettro di situazioni giuridiche riguardanti i videogiochi competitivi»: v. A. Maietta, *Gli e-sports,* cit.

[37] La proposta di legge n. 868 quantifica il fenomeno in circa 20 milioni di fatturato in Italia, con migliaia di utenti, 150 sale e innumerevoli competizioni.

[38] V. disegno di legge n. 970.

elettronici sono molteplici e concernono la qualificazione giuridica della prestazione lavorativa svolta, il riconoscimento delle variegate figure professionali del settore e-sportivo, la promozione di tutele adeguate sia in campo economico che nella protezione dell'integrità psicofisica di coloro che svolgono professionalmente l'attività di *gaming*, nonché il rischio di un forte squilibrio di genere.

Il nodo più intricato da sciogliere riguarda proprio chi, nel settore delle competizioni videoludiche, possa essere considerato lavoratore.

La risoluzione del Parlamento europeo appare piuttosto timida al riguardo. Al punto F dei *consideranda* riconosce che nel 2020 l'industria dei videogiochi ha occupato circa 98.000 persone in Europa[39], ma al punto 24 si limita ad invitare la Commissione e gli Stati membri a collaborare con le parti sociali per migliorare le condizioni di lavoro di «tutti coloro che sono coinvolti nello sviluppo dei videogiochi». Salvo che non si intenda adottare un'interpretazione estensiva, pare che il Parlamento Europeo si preoccupi di «garantire contratti equi e il rispetto della legislazione nazionale e dell'UE in materia di diritti dei lavoratori, equità e parità di retribuzione, salute fisica e mentale e sicurezza sul lavoro» soltanto ai *game developers*, ossia agli informatici, programmatori elettronici e ingegneri che realizzano e collaudano le applicazioni videoludiche. L'interpretazione restrittiva sembra avvalorata dal richiamo del Parlamento europeo[40] agli orari di lavoro «*crunch*»[41], che si verifica quando i dipendenti – in particolar modo programmatori e collaudatori di *software* – svolgono orari di lavoro prolungati, effettuando numerose ore di lavoro straordinario, spesso senza un adeguato compenso o senza rispettare i necessari tempi di riposo[42], per completare un progetto entro una scadenza rigida. Tali periodi *crunch* possono protrarsi anche per alcuni mesi[43], sottoponendo i lavoratori a uno stress prolungato, suscettibile di elevati rischi psicosociali.

Alla luce delle allarmanti conseguenze di tali dinamiche lavorative e delle necessarie tutele da approntare per evitarle, è pienamente comprensibile che la risoluzione europea si soffermi sulla figura degli sviluppatori di contenuti videoludici. Ciò che lascia perplessi è l'assenza di riferimenti alla figura del *gamer* professionista, ossia del soggetto che partecipa alle competizioni e-sportive in modo continuativo e professionale, percependo un reddito per la prestazione svolta.

Tale figura, nel settore degli sport elettronici, viene definita *pro-player*, ossia giocatore professionista, per distinguerlo da coloro che utilizzano i videogiochi soltanto come intrattenimento ludico.

Sotto questo profilo il disegno di legge italiano n. 970 fa un passo in avanti rispetto alla risoluzione europea, ammettendo che la partecipazione a competizioni videoludiche

---

[39] Il dato è riportato da ISFE, *Europe's Video Games Industry*, ISFE-EGDF Key Facts, 2021.

[40] Sempre nel punto 24 della risoluzione.

[41] Il c.d. *crunch effect* non è sostenibile a lungo termine e può comportare un esaurimento fisico e mentale del lavoratore.

[42] Un sondaggio condotto nel 2019 dalla *International Game Developers Association* ha rilevato che il 40% degli sviluppatori di *software* per l'industria videoludica ha lavorato nell'anno precedente almeno venti ore in più rispetto alla settimana lavorativa standard di quaranta ore e solo l'8% ha ricevuto un compenso aggiuntivo per quelle ore: v. C. Arnold, *Il video-sfruttamento*, in *Jabobin Italia*, 23 ottobre 2023.

[43] Nel 2019, lo sviluppatore David Brevik ha dichiarato che il *crunch* relativo al videogioco *Diablo* è durato dagli otto ai nove mesi, mentre quello per *Diablo II* è durato un anno e mezzo.

possa considerarsi lavoro vero e proprio. Al riguardo, distingue tra giocatore amatoriale – il quale gioca esclusivamente per diletto, senza alcun guadagno – e giocatore professionista.

La distinzione tra *gamer* occasionale e *gamer* abituale o, *rectius*, professionale è rilevante per le inevitabili ricadute in termini di regolamentazione e tutele giuslavoristiche: mentre il secondo si configura come lavoratore e, di conseguenza, è titolare di specifiche protezioni, il primo necessita di ben altro tipo di disciplina, relativa, ad esempio, alla corretta erogazione dei premi in palio per i vincitori delle competizioni videoludiche[44], a maggior ragione se avviene tramite criptovalute[45].

Per agevolare tale distinzione, la proposta di legge italiana n. 868 prevede l'istituzione presso il CONI di un Registro ufficiale delle associazioni, delle società e delle imprese e-sportive. L'iscrizione al registro sarebbe obbligatoria per svolgere le attività e-sportive[46]. Si tratterebbe di un adempimento – ricalcato sulla normativa in materia di enti sportivi professionistici e dilettantistici[47] – indispensabile per garantire la trasparenza e la tracciabilità nel settore degli *e-Sports*. A doversi iscrivere non sarebbe il singolo giocatore, ma l'associazione, società o impresa e-sportiva.

Anche il disegno di legge n. 970 prevede una registrazione[48], ma la prospettiva è leggermente diversa, in quanto onerati di tale adempimento sarebbero esclusivamente i soggetti che intendano organizzare una o più competizioni videoludiche in Italia, anche collegate tra loro, quali tornei e campionati, in presenza o a distanza, che prevedano la corresponsione di premi in denaro o sottoforma di beni o servizi dal valore superiore a € 2.500,00.

Di eventuali registri o registrazioni a livello europeo o di Stato membro non c'è traccia nella citata risoluzione UE. Eppure, anche in considerazione della portata transnazionale delle competizioni, potrebbe essere opportuna un'armonizzazione delle discipline in materia. Anche se lo sport – e, *a fortiori*, l'attività e-sportiva – non rientra tra le materie di competenza esclusiva o concorrente dell'Unione Europea, si tratta comunque di un settore destinatario delle misure «intese a sostenere, coordinare o completare l'azione degli Stati membri»[49].

---

[44] In assenza di una regolamentazione specifica per gli *e-Sport*, si ritengono applicabili alle competizioni videoludiche le disposizioni normative vigenti per le manifestazioni a premi, ossia il d.P.R. 26 ottobre 2001, n. 430, in caso di torneo con assegnazione di vincita non in denaro e il d. lgs. 14 aprile 1948, n. 496, relativo ai giochi di abilità a distanza con vincita in denaro, con l'applicabilità della complessa disciplina del gioco d'azzardo.

[45] Per un approfondimento sul punto, v. C. Pernice, *E-Sport e criptoattività: interazioni, regole e prospettive*, in A. Fuccillo - V. Nuzzo - M. Rubino De Ritis (a cura di), *Diritto e universi paralleli,* cit.*,* 3.

[46] Art. 13 della proposta di legge n. 868.

[47] A norma dell'art. 10 d. lgs. 28 febbraio 2021, n. 36, le associazioni e società sportive dilettantistiche sono riconosciute, ai fini sportivi, dalle Federazioni Sportive Nazionali, dalle Discipline Sportive Associate, dagli Enti di Promozione Sportiva.
La certificazione avviene mediante l'iscrizione nel Registro nazionale delle attività sportive dilettantistiche, tenuto dal Dipartimento per lo sport.

[48] Presso il Ministero della cultura.

[49] Art. 6 Trattato sul Funzionamento dell'UE.

4.1. Il *pro-player* e le affinità con il lavoro sportivo

I richiami al Registro e alle associazioni e società e-sportive presenti nella proposta di legge n. 868 non sono tentativi isolati di collegare la disciplina dell'attività videoludica alla regolamentazione del lavoro sportivo.

Anche il Codice degli *Esport* emanato dalla Repubblica di San Marino con legge 9 maggio 2023, n. 80, dopo aver definito, all'art. 4, il "giocatore professionista" come colui che svolge attività e-sportiva a titolo oneroso e in modo continuativo e prevalente rispetto ad altri impieghi o professioni e/o è classificato come tale per chiara fama nell'ambito della relativa disciplina e-sportiva, si sofferma sulla distinzione tra prestazione e-sportiva professionistica, dilettantistica e amatoriale[50], così come avviene nel settore sportivo.

Indubbiamente, le affinità tra i due settori sono molte e, in assenza di una specifica regolamentazione, la disciplina normativa dedicata allo sport sembrerebbe quella più appropriata.

Il d.lgs. n. 36/2021, che ha riordinato e riformato[51] le disposizioni in materia di enti sportivi professionistici e dilettantistici, nonché di lavoro sportivo, sembra confermare questa convergenza, dal momento che, all'art. 2, c. 1, lett. nn), assimila allo sport «qualsiasi forma di attività fisica fondata sul rispetto di regole che, attraverso una partecipazione organizzata o non organizzata, ha per obiettivo l'espressione o il miglioramento della condizione fisica e psichica, lo sviluppo delle relazioni sociali o l'ottenimento di risultati in competizioni di tutti i livelli».

Il riconoscimento degli *e-Sport* nell'ambito delle discipline sportive rappresenterebbe un importante passo in avanti nella loro promozione e regolamentazione, assicurando l'applicazione di tutto l'ordinamento sportivo – ormai collaudato in Italia da oltre quaranta anni – e le conseguenti tutele per i vari soggetti coinvolti[52].

Un altro segnale incoraggiante in questa direzione è la firma di un protocollo d'intesa[53] tra il CONI e il Comitato Promotore E-Sports Italia. Nel protocollo, il termine *E-sport* si riferisce «all'utilizzo di videogiochi sportivi a livello organizzato e competitivo» e comprende sia gli sport (o giochi) elettronici, «tramite i quali un determinato sport viene simulato attraverso l'utilizzo di varie interfacce videografiche […] con un minimo dispendio di energie fisiche, ma con un coinvolgimento generalmente medio-alto di quelle mentali», sia gli sport simulati, «tramite i quali un determinato sport viene simulato attraverso un utilizzo congiunto di interfacce video-grafiche […] e di strumenti che replicano l'attrezzo sportivo reale».

Benché tale Protocollo d'intesa non comporti il riconoscimento ai fini sportivi, né consenta l'inclusione nell'Elenco delle Discipline Sportive ammissibili per l'iscrizione al Registro C.O.N.I., la finalità principale è quella di incrementare la conoscenza e la diffusione delle attività e-sportive. In ogni caso, la sottoscrizione di un protocollo con il C.O.N.I. costituisce un avvicinamento importante tra i due settori, così come la pro-

[50] Rispettivamente, artt. 13, 14 e 15.

[51] Ha abrogato, tra le altre, la l. 23 marzo 1981, n. 90, sul professionismo sportivo.

[52] OIES, *White Paper Esports e gaming in Italia 2023*, cit.

[53] Il 14 gennaio 2022.

posta lanciata dal Comitato Olimpico Internazionale di creare degli *Olympic E-sports Games*[54].

D'altronde, il 7 luglio 2021 il *Sim Racing* – termine che indica competizioni di *e-Sport* con *software* che tentano di simulare accuratamente le corse automobilistiche, finanche includendo le variabili riconducibili all'esperienza concreta, quali il consumo di carburante, i danni, l'usura e l'aderenza degli pneumatici, nonchè le impostazioni delle sospensioni – è stato inserito all'interno dell'elenco delle discipline sportive ammissibili per l'iscrizione al Registro Nazionale delle Associazioni e Società Sportive Dilettantistiche[55]. Per la precisione, è stato collocato nell'area sportiva dedicata all'automobilismo, di competenza, sul territorio nazionale, della federazione Automobile Club d'Italia[56]. In tale disciplina e-sportiva l'Italia risulta particolarmente abile e competitiva, come dimostrano i brillanti risultati conseguiti a livello mondiale[57].

L'estensione delle tutele sportive agli sport elettronici potrebbe senz'altro agevolare ed accelerare il riconoscimento di tutele e garanzie ai *pro-player*, che verrebbero equiparati agli atleti[58], con la relativa protezione in caso di giocatori minorenni[59], sia cittadini UE che extra-UE.

I minorenni, infatti, rappresentano una percentuale significativa dei *pro-player*[60] e questo dato sollecita particolare attenzione. Da un lato, il Commento generale n. 25 del 2021 sui diritti del fanciullo nell'ambiente digitale[61] evidenzia come le tecnologie digitali siano «vitali» per la crescita e il futuro dei bambini e degli adolescenti[62]; dall'altro, però, la predisposizione dei ragazzi al gioco e la loro disponibilità di tempo libero, spesso trascorso davanti a una *console*, li espone a seri rischi. Nel settore videoludico, il confine tra gioco e lavoro è particolarmente labile e i più giovani, senza la previsione di adeguate tutele, possono trovarsi coinvolti in meccanismi rischiosi, come attesta la circostanza che, nel 2020, un bambino di soli otto anni sia stato ingaggiato in qualità di *pro-player* da una squadra americana di sport elettronici al fine di partecipare alle

[54] V. *Parigi 2024, il CIO proporrà le Olimpiadi degli Esports*, in *Corriere dello Sport*, 17 giugno 2024.

[55] V. R. Di Lenola, *Il Coni aggiorna l'elenco delle discipline sportive riconosciute,* in *Gruppo Sportivo Italiano,* 1 agosto 2021.

[56] V. *ACI Sport*, 21 luglio 2021.

[57] L'Italia può vantare i migliori *simdrivers* al mondo. La medaglia d'oro alle prime *Olympic Virtual Series* nella categoria Motorsport, disputate a Tokio nel 2021, è stata vinta da un italiano, Valerio Gallo. Nell'edizione successiva, svoltasi a Singapore nel 2023, l'italiano Giorgio Mangano si è qualificato al primo posto, dopo aver sbaragliato oltre 160.000 partecipanti provenienti da 66 Paesi nel mondo. V. *L'italiano Mangano primo classificato alle Olimpiadi dell'Esports*, in *Tutto Sport*, 11 maggio 2023.

[58] Art. 15 d. lgs. 36/2021.

[59] Art. 16 d. lgs. 36/2021.

[60] OIES, *White Paper Esports e gaming in Italia 2023*, cit.

[61] Adottato dal Comitato delle Nazioni Unite sui Diritti dell'Infanzia.

[62] In tal senso, v. già l'art. 31 della Convenzione dei diritti del fanciullo, approvata dall'Assemblea Generale delle Nazioni Unite il 20 novembre 1989 e ratificata dall'Italia il 27 maggio 1991, che riconosce ai ragazzi il diritto a dedicarsi al gioco e alle attività ricreative.

competizioni del videogioco *Fortnite*[63]. Pur rientrando in uno dei settori[64] per i quali, in Italia[65], sono consentite le deroghe al lavoro degli infrasedicenni[66], tali situazioni andrebbero accuratamente disciplinate per assicurare al fanciullo l'assolvimento dell'obbligo scolastico e il rispetto dei tempi di riposo a tutela della sua integrità psicofisica[67]. Inoltre, il *team* o la Federazione di riferimento dovrebbe assicurarsi che il giocatore minorenne non pratichi discipline *e*-sportive che presentino una classificazione *Pan European Game Information*[68] incompatibile con la sua età[69].

Qualche dubbio, però, potrebbe sorgere sull'estensione delle tutele sportive alle competizioni videoludiche che non concernono simulazioni di attività sportive e non richiedano neppure una minima attività fisica[70]. Il mondo dei videogiochi è estremamente ampio e variegato, contemplando diverse tipologie, oltre a quella sportiva, come attestano i numerosi giochi di avventura, di ruolo, di strategia, ecc.

Un'interpretazione restrittiva potrebbe escludere queste categorie di videogiochi – che non hanno alcuna assonanza con le discipline sportive esistenti – dal novero degli sport elettronici. Eppure, una più accurata riflessione sulle finalità dei videogiochi generalmente intesi – sviluppo delle abilità sensoriali e della coordinazione occhio-mano, potenziamento dell'apprendimento e del *problem solving*[71], miglioramento delle capacità sociali[72] – consentirebbe di considerarli comunque «sport della mente»[73]. Tale lettura appare anche pienamente compatibile con il settimo comma dell'art. 33 Cost.[74], che «riconosce il valore educativo, sociale e di promozione del benessere psicofisico dell'attività sportiva in tutte le sue forme». Nell'espressione «in tutte le sue forme» potrebbero, appunto, rientrare anche le attività e-sportive.

---

[63] Joseph Dean ha ricevuto dal *Team* californiano 33 un compenso di $ 33.000 e un pc ad alte prestazioni per lo svolgimento della sua attività professionistica di *gamer:* J. Tidy, *Fortnite: From piano player to pro gamer - aged just eight,* in *BBC*, 2 marzo 2021.

[64] Se anche non si volesse riconoscere la natura sportiva della prestazione e-sportiva, potrebbe comunque rientrare tra le attività di carattere culturale.

[65] Art. 4, c. 2, l. 17 ottobre 1977, n. 977 e s.m.i.

[66] In ogni caso è richiesto il consenso scritto dei genitori e l'autorizzazione dell'Ispettorato del lavoro territorialmente competente.

[67] Cfr. art. 33, c. 6, d. lgs. 36/2021 per i lavoratori sportivi minori. V. art. 37, c. 2, Cost. e il combinato disposto tra l'art. 3 l. 17 ottobre 1967, n. 977 e l'art. 1, c. 662, l. 27 dicembre 2006, n. 296.

[68] Si tratta di un metodo di classificazione adottato dal 2003 in Europa per suddividere i videogiochi in cinque categorie di età e otto descrizioni di contenuto.

[69] Sul punto, v. art. 10, c. 4, della proposta di legge n. 868.

[70] Al riguardo, può risultare interessante la sentenza della CGUE, C-90/16, *The English Bridge Union Limited* (2017), la quale, a fini dell'applicazione della direttiva sull'IVA, ha stabilito come il gioco del bridge duplicato (la versione del bridge generalmente utilizzata nelle competizioni) non possa essere considerato uno sport. Secondo la Corte europea, per ottenere lo *status* di sport, un'attività deve prevedere «una componente fisica non irrilevante».

[71] M. Patenaude, *Playing action video games can boost learning*, in *University of Rochester*, 10 novembre 2014.

[72] Riducendo, ad esempio, le reazioni violente o aggressive. Sul punto, N. L. Carnagey - C. A. Anderson - B. J. Bushman, *The effect of video game violence on physiological desensitization to real-life violence*, in *Journal of Experimental Social Psychology*, 4, 2007, 684 ss.

[73] OIES, *White Paper Esports e gaming in Italia 2023*, cit. Al riguardo, si pensi ai c.d. *games for the brain*, tra i quali il sudoku, wordle, tetris…

[74] Comma introdotto dall'art. 1, c. 1, l. cost. 26 settembre 2023, n. 1.

4.2. La qualificazione giuridica della prestazione e-sportiva

Il disegno di legge n. 970, come visto, considera il giocatore professionista un prestatore di lavoro, e, all'art. 2, c. 1, lett. h), lo definisce come «qualsiasi persona fisica per la quale la partecipazione a competizioni videoludiche costituisca svolgimento di un'attività economica, condotta in modo continuativo o con finalità di lucro, nel contesto di un rapporto di lavoro subordinato, autonomo od occasionale, con una squadra».
Si tratta di una descrizione piuttosto ampia, che non fornisce alcuna indicazione in merito alla tipologia contrattuale da utilizzare, come se nell'ambito e-sportivo fossero fungibili o equivalenti.
La questione è delicata e merita qualche riflessione ulteriore.
Innanzitutto, dovremmo chiederci se per individuare la natura giuridica della prestazione lavorativa svolta dal *pro-player* valgano gli stessi – dibattuti e, talvolta, controversi – indici giurisprudenziali adottati per le forme di lavoro comuni oppure se la scelta più opportuna sia estendere le categorie previste per la disciplina speciale del lavoro sportivo.
La specialità del lavoro sportivo[75] è chiaramente affermata dal c. 1-*bis* dell'art. 25 d. lgs. n. 36/2021: «La disciplina del lavoro sportivo è posta a tutela della dignità dei lavoratori nel rispetto del principio di specificità dello sport»[76].
La riforma dei rapporti di lavoro in ambito sportivo[77], introdotta dal d. lgs. n. 36/2021, è entrata in vigore il primo luglio 2023[78] ed è ancora in fase di assestamento, come dimostra l'emanazione del d.l. 31 maggio 2024, n. 71, recante, tra le altre, disposizioni urgenti in materia di sport.

---

[75] Tale specialità si riverbera nelle numerose deroghe alla disciplina generale in materia di lavoro subordinato, introdotte dall'art. 26 d. lgs. 36/2021: ad es., in materia controlli a distanza (art. 4 Stat. Lav.) e di accertamenti sanitari (art. 5 Stat. Lav.), di licenziamenti, di durata del contratto a tempo determinato. In dottrina, di recente, v. C. De Martino, *La specialità del lavoratore sportivo. Nozioni, tipi contrattuali, disciplina e tutele*, Bari, 2024.

[76] Sul punto, v. A.L. Fraioli, *La riforma del lavoro sportivo di cui al d. lgs. n. 36/2021*, in *Massimario di Giurisprudenza del Lavoro*, 1, 2023, 55.

[77] Per un'ampia disamina v. M. Biasi, *Causa e tipo nella riforma del lavoro sportivo. Brevi osservazioni sulle figure del lavoratore sportivo e dello sportivo amatore nel d.lgs. n. 36/2021*, in *Lavoro Diritti Europa*, 3, 2021; C. Di Mattina, *Il rapporto di lavoro sportivo. La riforma del lavoro sportivo aggiornata al decreto correttivo-bis (D. Lgs. n. 120/2023)*, Milano, 2023; G. Liotta - L. Santoro*, Lezioni di Diritto Sportivo*, Milano, 2023; T. Vettor, *La nuova riforma del lavoro sportivo: prime analisi alle disposizioni integrative e correttive al d.lgs. n. 36/2021 (d.lgs. n. 163/2022)*, in *Massimario di Giurisprudenza del Lavoro*, 1, 2023, 129; S. Bellomo - G. Capilli - M. A. Livi - D. Mezzacapo - P. Sandulli, *Lineamenti di diritto sportivo*, Torino, 2024; M. Biasi, *Universalismo vs. selettività nel diritto del lavoro sportivo: Italia e Stati Uniti a confronto*, in *Variazioni su Temi di Diritto del Lavoro*, 2, 2024, 387; P. Lambertucci, *Il lavoro sportivo subordinato tra disciplina speciale e normativa generale di tutela: prime considerazioni sulla riforma del 2021*, in *Argomenti di Diritto del Lavoro*, 1, 2024, 1; R. Nunin, *Introduzione. La riforma del lavoro sportivo: un intervento atteso, complesso, discusso*, in *Variazioni su Temi di Diritto del Lavoro*, 2, 2024, 286; A. Trojsi, *La riforma del lavoro sportivo nel sistema delle fonti*, in *Lavori Diritti Europa*, 3, 2024; T. Vettor, *La riforma dello sport. Valori, principi e diritti nella prospettiva del lavoro*, in *Variazioni su Temi di Diritto del Lavoro*, 2, 2024, 293.

[78] L'entrata in vigore della riforma è avvenuta a tappe: alcune disposizioni sono entrate in vigore il primo gennaio 2022, quelle relative alla disciplina dei rapporti di lavoro sportivo il primo luglio 2023, alcuni adempimenti relativi alle società sportive professionistiche (art. 13, c. 7, d. lgs. 36/2021) entreranno in vigore il primo luglio 2025: v. art. 51 d. lgs. 36/2021.

La nuova disciplina denomina "lavoratore sportivo" non soltanto l'atleta, ma ogni figura coinvolta nel settore sportivo (l'allenatore, l'istruttore, il direttore tecnico, il direttore sportivo, il preparatore atletico e il direttore di gara), che, senza alcuna distinzione di genere e «indipendentemente dal settore professionistico o dilettantistico»[79], esercita l'attività sportiva verso un corrispettivo[80] a favore di un soggetto iscritto nel Registro nazionale delle attività sportive dilettantistiche, nonché a favore delle Federazioni sportive nazionali, delle Discipline sportive associate, degli Enti di promozione sportiva, delle associazioni benemerite, anche paralimpici, del CONI, del CIP e di Sport e salute S.p.a. o di altro soggetto tesserato.

Ciò che caratterizza l'inserimento del lavoratore sportivo nell'area del professionismo o del dilettantismo è l'appartenenza a una società professionistica[81] o a un'associazione o società dilettantistica[82]. Quindi, la distinzione non riguarda le modalità di svolgimento della prestazione lavorativa, ma la natura – professionistica o dilettantistica – dell'ente sportivo con il quale viene sottoscritto il contratto di lavoro sportivo. In considerazione del fatto che in Italia, delle 387 discipline sportive riconosciute, soltanto quattro sono sport professionistici[83] (calcio[84], golf, pallacanestro[85] e ciclismo), la maggior parte dei lavoratori sportivi rientra nell'area dilettantistica.

L'attività di lavoro sportivo può costituire oggetto di un rapporto di lavoro subordinato o di un rapporto di lavoro autonomo, anche nella forma di collaborazioni coordinate e continuative[86], ma il lavoro sportivo prestato dagli atleti[87] nei settori professionistici[88] «si presume oggetto di contratto di lavoro subordinato»[89], mentre per quello esercitato nell'area del dilettantismo vige la presunzione di «lavoro autonomo,

[79] Art. 25, c. 1, d. lgs. 36/2021.

[80] I volontari, invece, sono coloro che mettono a disposizione il proprio tempo e le proprie capacità per promuovere lo sport, in modo personale, spontaneo e gratuito, senza fini di lucro, neanche indiretti, ma esclusivamente «con finalità amatoriali». Si tratta dei soggetti che svolgono attività sportiva per hobby e non vengono retribuiti in alcun modo, salvo il riconoscimento di rimborsi forfettari per le spese sostenute per le attività svolte, nel limite complessivo di 400 euro mensili, in occasione di manifestazioni ed eventi sportivi riconosciuti dalle Federazioni sportive nazionali: v. art. 29 d. lgs. 36/2021.

[81] A norma dell'art. 13 d. lgs. 36/2021, le società sportive professionistiche sono costituite nella forma di società per azioni o di società a responsabilità limitata.

[82] L'area del dilettantismo comprende le associazioni e le società, inclusi gli enti del terzo settore, che svolgono attività sportiva in tutte le sue forme, con prevalente finalità altruistica, ossia senza fine di lucro, ai sensi dell'art. 8 d. lgs. 36/2021.

[83] In cui sono presenti società professionistiche.

[84] Per quanto riguarda il calcio femminile, è opportuno ricordare che rientra nell'area del professionismo soltanto a partire dal primo luglio 2022 e limitatamente alla serie A.

[85] Soltanto la Lega Basket Serie A.

[86] V. art. 25, c. 2, d. lgs. 36/2021.

[87] Il fatto che la presunzione della natura subordinata del rapporto sia circoscritta ai soli atleti deriva dall'art. 3 della l. 91/1981 ed è avvalorata da Cass. civ., sez. lav., 1 agosto 2011, n. 16849, secondo cui, per le altre figure di lavoratori sportivi, la sussistenza del vincolo di subordinazione deve essere accertata di volta in volta nel caso concreto, in applicazione dei criteri forniti dal diritto comune del lavoro. In tal senso, v. anche Cass. civ., sez. lav., 28 dicembre 1996, n. 11540.

[88] Come attività principale, ovvero prevalente, e continuativa.

[89] Art. 27, c. 2, d. lgs. 36/2021.

nella forma della collaborazione coordinata e continuativa»[90]. Inoltre, ai sensi del c. 3-*bis* dell'art. 25 d. lgs. 36/2021, le associazioni e società sportive «possono avvalersi di prestatori di lavoro occasionale, secondo la normativa vigente».

Dal riconoscimento della natura subordinata o autonoma del rapporto discendono, ovviamente, tutele diversificate: al riguardo sono esemplificativi, sotto il profilo previdenziale, l'art. 35, commi 1 e 2 – sul trattamento pensionistico, rispettivamente, dei lavoratori sportivi subordinati e di quelli titolari di contratti di collaborazione coordinata e continuativa – e l'art. 33, commi 3-5, sulle tutele per la maternità, la malattia, gli assegni per il nucleo familiare e la NASpI.

Questo breve *excursus* sull'ampia e variegata disciplina dei rapporti sportivi è indispensabile per interrogarsi sulla possibilità e opportunità di estenderla *tout court* al settore e-sportivo, al fine di colmare la lacuna di regolamentazione specifica. Al momento non appare percorribile la strada della sua applicazione analogica, stante la specialità della disciplina sportiva. Diversa sarebbe la situazione se gli *e-Sport* venissero riconosciuti come discipline sportive: in tal caso verrebbero pacificamente estese tutte le tutele previste per l'attività sportiva svolta in modo professionale. Lascia, perciò, perplessi la circostanza che una così recente riforma sul lavoro sportivo non abbia preso in considerazione gli *e-Sports*, nonostante la loro ormai consolidata diffusione e le forti assonanze con l'attività sportiva. Si tratta di una vera e propria occasione mancata.

Rebus sic stantibus, non possono che applicarsi al *pro-player* i tradizionali indici di subordinazione, riconoscendo, caso per caso, la natura subordinata o autonoma della prestazione in base alle concrete modalità di svolgimento della prestazione. Secondo il *White Paper* presentato dall'Osservatorio Italiano *E-Sports*, «la qualificazione della prestazione del *gamer* come attività di lavoro autonomo sembra essere quella giuridicamente più corretta»[91], in quanto difficilmente sarebbe ravvisabile il vincolo di subordinazione. In realtà, tale affermazione non è pienamente condivisibile, perché la qualificazione giuridica della prestazione non può essere valutata astrattamente, bensì analizzata alla luce del concreto rapporto posto in essere tra il *pro-player* e il *team* con il quale ha sottoscritto il contratto. Potrebbero essere considerati indici di subordinazione, ad esempio, l'individuazione di un numero predeterminato di ore giornaliere di allenamento (anche con possibilità di verifica da parte della squadra mediante l'utilizzo condiviso della piattaforma), l'imposizione dell'obbligo di partecipazione a riunioni – anche svolte da remoto – per la definizione di tattiche e strategie, nonché la corresponsione di un importo mensile fisso a prescindere dal numero di partecipazioni a competizioni o dai premi conseguiti.

La questione, pertanto, è ancora aperta, lasciando troppe zone d'ombra che rischiano di mettere a repentaglio la dignità del lavoratore e-sportivo.

[90] Art. 28, c. 2, d. lgs. 36/2021, purché le prestazioni oggetto del contratto non superino le ventiquattro ore settimanali e siano «coordinate sotto il profilo tecnico-sportivo».

[91] OIES, *White Paper Esports,* cit., 20.

4.3. La tutela della salute psicofisica del *pro-player*

Un'altra criticità da prendere in esame è l'individuazione delle modalità più efficaci per garantire la tutela della salute psicofisica del *pro-player*, in quanto quotidianamente esposto a innumerevoli e diversificati rischi[92], le cui ripercussioni possono rivelarsi gravi e durature.

Ad esempio, le lunghe sessioni di allenamento, nonché l'accanimento e la tensione con cui vengono affrontate le competizioni virtuali comportano la prolungata assunzione di posture statiche e innaturali[93] e il conseguente sviluppo di dolori cervicali, tensioni muscolari e limitazioni articolari. Questo *mix* di fattori ha assunto la denominazione di cervicalgia da *gaming* e può accompagnarsi alla lombalgia e al mal di testa muscolo-tensivo[94].

Anche il *gamer's thumb* è un rischio ricorrente per il *pro-player,* che impugna il *joystick* per molte ore al giorno. Da tale problematica sono interessati due tendini del polso e della mano e i sintomi più ricorrenti sono il dolore al pollice e al polso e la riduzione di forza nella presa.

Alle patologie tipiche si aggiungono quelle eventuali, quali l'alterazione della postura e l'affaticamento della vista, lamentati da oltre il 25% dei *gamers*[95].

I più insidiosi, però, sono i rischi psicosociali connessi all'abuso delle tecnologie digitali utilizzate. Senza le opportune cautele, l'attività svolta dal *pro-player* potrebbe portare alle estreme conseguenze i seri rischi già segnalati in dottrina per il lavoro digitale[96] generalmente inteso: l'elevato livello di stress lavoro correlato, suscettibile di sfociare nel *burnout*, nonché il senso di isolamento[97], perché il giocatore può sentirsi intrappolato in una relazione esclusiva con il videogioco. D'altronde, l'Organizzazione Mondiale della Sanità (OMS) ha riconosciuto ufficialmente la dipendenza da *videogame* come una patologia, denominata *gaming disorder*, recentemente inserita tra le oltre 55.000 patologie mentali[98]. La dipendenza si manifesta in una serie di comportamenti persistenti che attribuiscono una crescente priorità al gioco rispetto alle altre attività e agli interessi quotidiani e che continuano o, addirittura, si intensificano nonostante il verificarsi di conseguenze negative. Uno degli effetti ricorrenti è proprio l'incapacità di "staccare"[99], non riuscendo, così, a fruire dei necessari tempi di riposo psicofisico. La

---

92 Sul punto, v. C. Di Carluccio, *E-sport, lavoro e salute. Note sulla condizione del pro-player*, in G. Bevilacqua - A. Lepore, *Sport elettronici, sicurezza e diritti umani*, in *Quaderni della Rassegna di diritto ed economia dello Sport,* 2024, 61.

93 Ad esempio, il capo protratto in avanti, le spalle ruotate all'interno, la testa e il collo inclinati.

94 V. *Cervicalgia da gaming: le cause, come curarla e prevenirla,* in *Pro2be,* 23 giugno 2021.

95 V. A. Citterio, *Gaming e postura*, in *Studio Volta Milano*, 8 settembre 2022.

96 Eurofound-ILO, *Working anytime anywhere,* cit., 33; A. Fenoglio, *Il tempo di lavoro nella new automation age: un quadro in trasformazione*, in *Rivista Italiana di Diritto del Lavoro*, 4, 2018, 625; M. Pilotto - R. Salomone, *Stress lavoro-correlato: primi spunti per un dialogo tra diritto e psicologia del lavoro*, in *Giornale italiano di psicologia*, 1-2, 2019, 147.

97 Eurofound-ILO, *Working anytime anywhere,* cit., 37.

98 Dal primo gennaio 2022 è stato inserito nell'*International Classification of Diseases* (ICD).

99 Sulla disconnessione v. E. Dagnino, *Il diritto alla disconnessione nella legge n. 81/2017 e nell'esperienza comparata*, in *Diritto delle Relazioni Industriali*, 4, 2017, 1024; R. Zucaro, *Il diritto alla disconnessione tra interesse*

situazione è ancora più allarmante se si considera l'elevato numero di minori coinvolti nell'attività di *pro-player*[100].

Anche in assenza di una regolamentazione *ad hoc* per i lavoratori e-sportivi, è ragionevole ritenere che non possa sussistere una zona franca, un *far west* senza alcuna misura preventiva nei confronti di coloro che esercitano una prestazione lavorativa, per quanto nell'ambito di un settore di nicchia.

D'altronde, alla luce dell'art. 2087 c.c., norma cardine sugli obblighi di sicurezza gravanti in capo al datore di lavoro, «l'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro». Al riguardo, è opportuno ricordare che il d. lgs. 9 aprile 2008, n. 81, c.d. Testo unico in materia di salute e sicurezza sul lavoro, definisce lavoratore – e, quindi, soggetto destinatario delle misure protettive ivi previste – la «persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa»[101] e datore di lavoro – principale responsabile della fitta trama di misure preventive e protettive – «il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa»[102].

Tra le varie tutele previste dal d. lgs. n. 81/2008, dovrebbero senz'altro essere prese in considerazione quelle rivolte ai videoterminalisti: date le caratteristiche dell'attività svolta dal *pro-player*, non c'è dubbio che possa rientrare tra quelle effettuate davanti a «uno schermo alfanumerico o grafico a prescindere dal tipo di procedimento di visualizzazione utilizzato»[103], utilizzando un «sistema di immissione dati, incluso il *mouse*, il *software* per l'interfaccia uomo-macchina, gli accessori opzionali, le apparecchiature connesse»[104]. Alla luce dei rischi specifici per l'esecuzione della prestazione al videoterminale, il datore di lavoro non potrà non tenere conto delle condizioni ergonomiche, dei problemi legati alla vista, alla postura e all'affaticamento fisico e mentale[105], nonché delle modalità atte a consentire il rispetto dei tempi di riposo.

Inoltre, nell'attività del *pro-player* assumono grande rilevanza sia l'adeguatezza ed efficienza degli strumenti digitali utilizzati sia la stabilità e potenza della connessione Internet. È ragionevole che a farsi carico dell'assegnazione e della manutenzione di tali

collettivo e individuale. Possibili profili di tutela, in *Labour & Law Issues.*, 2, 2019, 215; M. Russo, *Esiste il diritto alla disconnessione?* cit., 682; M. Biasi, *Individuale e collettivo nel diritto alla disconnessione: spunti comparatistici*, in *Diritto delle Relazioni Industriali*, 2, 2022, 400; D. Calderara, *Garanzia della disconnessione nel rapporto di lavoro*, Torino, 2024; A. Rosanò, *Preparare lo scudo: considerazioni su intelligenza artificiale e diritto alla disconnessione a seguito dell'adozione del regolamento (UE) 2024/1689*, in questa *Rivista*, 2, 2024, 78.

100 V. *supra*, par. 4.1. Sul punto, v. C. Ghionni Crivelli Visconti, *E-sports e persone minori di età nell'ambiente digitale*, in G. Bevilacqua - A. Lepore (a cura di), *Sport elettronici, sicurezza e diritti umani*, cit., 107.

101 Art. 2, c. 1, lett. a), d. lgs. 81/2008.

102 Art. 2, c. 1, lett. b), d. lgs. 81/2008. Per un approfondimento, v. Aa. Vv., *Memento Pratico Salute e sicurezza sul lavoro*, Milano, 2024, 650 ss.

103 Art. 173, c. 1, lett. a), d. lgs. 81/2008.

104 Art. 173, c. 1, lett. b), d. lgs. 81/2008.

105 V. art. 174, c. 1, d. lgs. 81/2008.

strumenti di lavoro sia il *team* con il quale il *pro-player* ha sottoscritto il contratto di lavoro, qualunque sia la tipologia contrattuale adottata. In ogni caso, la regolamentazione di questo aspetto è fondamentale non soltanto per delineare con chiarezza il perimetro delle responsabilità in caso di malfunzionamento e conseguente infortunio, ma anche per verificare la conformità al T.U. in materia di sicurezza sul lavoro. Quest'ultimo definisce come attrezzatura di lavoro «qualsiasi macchina, apparecchio, utensile o impianto […] destinato ad essere usato durante il lavoro»[106] e stabilisce che sia il datore di lavoro a mettere «a disposizione dei lavoratori attrezzature […] idonee ai fini della salute e della sicurezza e adeguate al lavoro da svolgere»[107].

L'assolvimento degli obblighi in materia di sicurezza da parte del datore di lavoro richiede particolare attenzione nel caso di prestazione e-sportiva, la quale configura un esempio lampante di destrutturazione degli spazi di lavoro, potendo essere realizzata da qualsiasi luogo – che sia l'abitazione del *pro-player* o una c.d. sala LAN (Local Area Network)[108] – mediante l'impiego di dispositivi elettronici. E ulteriori cautele potrebbe richiedere il ricorso alle potenzialità sottese alla realtà virtuale, aumentata o mista dell'esperienza immersiva offerta dal metaverso[109], al fine di prevenire la possibile amplificazione dei rischi psicosociali sopra evidenziati.

Infine, è opportuno rilevare che, per quanto concerne le misure in materia di salute e sicurezza sul lavoro, non risulterebbe determinante l'estensione della disciplina prevista per i lavoratori sportivi, in quanto l'art. 33 d. lgs. 36/2021, rubricato "Sicurezza dei lavoratori sportivi e dei minori", si limita ad operare «un rinvio, per certi versi "acritico" alla disciplina generale»[110]. D'altronde, più che come oggetto della tutela della salute psicofisica dell'individuo, l'attività sportiva è considerata uno strumento prezioso per il suo sviluppo[111], come sottolinea il c. 7 dell'art. 33 Cost.[112].

---

[106] Art. 69, c. 1, lett. a), d. lgs. 81/2008.

[107] Art. 71, c. 1, d. lgs. 81/2008, rubricato "obblighi del datore di lavoro".

[108] Si tratta di spazi adibiti al *gaming* con la possibilità di operare in modalità *multiplayer* utilizzando, appunto, una rete LAN. L'utilizzo di queste sale è piuttosto controverso: nell'aprile 2022, l'Agenzia delle Dogane e dei Monopoli è intervenuta nei confronti di alcune sale LAN disponendone la chiusura e il sequestro dei dispositivi utilizzati, per violazione dell'art. 110, c. 9, lett. f-*quater* del T.U.L.P.S. A tale vicenda hanno fatto immediatamente seguito la circ. 19 maggio 2022, n. 18, la circ. 6 giugno 2022, n. 21, e la Determinazione direttoriale 10 giugno 2022, recanti chiarimenti e linee guida nell'utilizzo di tali sale e degli apparecchi ivi contenuti per finalità e-sportiva. Alla luce dell'attuale quadro regolamentare, le sale LAN dovrebbero essere qualificate come sale pubbliche da gioco ai sensi dell'art. 69 T.U.L.P.S.

[109] Sul metaverso, v. M. Ball, *Metaverso*, Milano, 2022; H. Narula, V*irtual Society. The Metaverse and the new frontiers of human experience*, New York, 2022; V. De Stefano - A. Aloisi - N. Countouris, *Il Metaverso è una questione di diritto, 2022,* in *socialeurope.eu;* A. Donini - M. Novella - M.L. Vallauri*, Prime riflessioni sul lavoro nel metaverso*, in *Labour & Law Issues,* 2022; M. Martone*, Prime riflessioni su lavoro e metaverso*, in *Argomenti di Diritto del Lavoro*, 2022, 1131; M. Biasi, *Il decent work e la dimensione virtuale: spunti di riflessione sulla regolazione del lavoro nel Metaverso,* in *Lavoro Diritti Europa,* 2023; M. Russo, *Le sfide nella regolamentazione del lavoro tecnologico: dal lavoro agile al metaverso*, in A. Fuccillo - V. Nuzzo - M. Rubino De Ritis (a cura di), *Diritto e universi paralleli,* cit.*,* 82; R. Bifulco, *Riverberi costituzionali del Metaverso*, in questa *Rivista*, 3, 2023.

[110] A. Delogu, *Alcune annotazioni sulla tutela della salute e sicurezza dei lavoratori nella riforma del lavoro sportivo*, in *Diritto della sicurezza sul lavoro*, 1, 2024, 25.

[111] Il report *Step up! Tackling the burden of insufficient physical activity in Europe*, pubblicato nel 2023 dall'OMS e dall'OCSE, con il supporto economico dell'Unione Europea, spiega come, aumentando la pratica di attività fisica, si potrebbero prevenire migliaia di morti premature e ridurre i costi della spesa sanitaria.

[112] In un primo momento, la tutela dello sport era stata inserita nell'art. 32 Cost. – anziché nell'art. 33

Nell'attività e-sportiva, invece, alla luce delle preoccupazioni più volte manifestate dall'OMS nei confronti dei rischi psicosociali e delle dipendenze collegate all'uso smodato dei videogiochi, i rischi potrebbero talvolta superare i benefici[113]. Ciononostante, il *White Paper* dell'OIES non affronta compiutamente le criticità collegate ai rischi psicofisici del *pro-player* e si limita a segnalare la necessità di un supporto psicologico e fisioterapico per chi svolge professionalmente attività e-sportiva. Ovviamente, la presenza di figure specializzate all'interno del *team* può contribuire a migliorare la salute fisica e mentale dei soggetti coinvolti, prevenendo il *gaming disorder* e promuovendo il benessere psicofisico[114], ma ciò non esclude la necessità di un'accurata valutazione dei rischi e la predisposizione di valide misure preventive.

5. Osservazioni conclusive e prospettive future

Gli *e-Sports* rappresentano indubbiamente una delle nuove frontiere della digitalizzazione del lavoro e la difficoltà nella loro regolamentazione è perfettamente comprensibile alla luce del delicato bilanciamento tra rapidità e multiformità del progresso tecnologico, da un lato, e garanzia dei diritti fondamentali della persona che lavora, dall'altro.

La "timidezza" legislativa nella regolazione degli *e-Sports* e dell'attività videoludica in generale[115] potrebbe anche essere letta come volontà di non ingerenza, al fine di evitare di comprimere o vincolare eccessivamente una realtà così dinamica e in continua evoluzione. O, comunque, potrebbe nascondere l'intenzione di restare in vigilante attesa di una sorta di assestamento della materia prima di intervenire a livello normativo.

L'assenza di una regolamentazione *ad hoc* per lo svolgimento professionale dell'attività e-sportiva rappresenta, però, un *deficit* di tutele per gli operatori del settore videoludico e, in modo particolare, per la figura del *pro-player*, sulla quale il presente contributo è focalizzato.

Alla luce delle criticità segnalate e dello stato dell'arte, è il caso di interrogarsi sulle prospettive regolatorie del fenomeno e-sportivo a breve, medio e lungo termine, a seconda degli scenari che potrebbero prospettarsi.

L'estensione *tout court* della disciplina prevista per il lavoro sportivo non appare, al momento, praticabile. Non si può ignorare il fatto che la legge delega 8 agosto 2019, n. 86

– proprio per sottolineare l'importanza dell'attività sportiva per il benessere dell'individuo e per la salute (v. proposta di legge costituzionale presentata il 21 marzo 2014). Successivamente, è stato preferito l'inserimento nell'art. 33 Cost., in materia di cultura e istruzione, per valorizzare la funzione educativa svolta dallo sport, soprattutto nei confronti dei giovani.

113 Secondo le Linee guida OMS del 2020 "*every move counts towards better health*". Anzi, l'attività e-sportiva rischia di «allontanare i minorenni dalle pratiche motorie e sportive»: P. Raimondo, *Sport vs esports. Una difficile convivenza*, in *Federalismi*, 1, 2022, 148.

114 OIES, *White Paper Esports,* cit., 98.

115 Oltre alla proposta di legge n. 868 e al disegno di legge n. 970, presentati nel corso della XIX legislatura, sono stati presentati il disegno di legge n. 2624 e le proposte di legge n. 3626 e n. 3679 durante la XVIII legislatura. Il tema è stato più volte sottoposto all'attenzione delle Camere, ma ancora non è stato approvato alcunché in materia. A livello sovranazionale, v. risoluzione del Parlamento EU del 10 novembre 2022.

e il d. lgs. n. 36/2021 non abbiano tenuto conto dell'attività e-sportiva, pur riformando il lavoro sportivo quando ormai la realtà degli sport elettronici si era già manifestata nella sua complessità e urgenza.

Eppure, le affinità tra i due settori sono numerose e i segnali di avvicinamento[116] sembrano incoraggianti. Alla luce di ciò, la soluzione più immediata e agevole potrebbe consistere nell'ennesima modifica al d. lgs. 36/2021, estendendo agli sport elettronici la disciplina e le tutele previste, ove compatibili. Ciò presupporrebbe, però, alcuni passaggi propedeutici, come il riconoscimento dell'attività videoludica ai fini sportivi e l'iscrizione nel Registro del CONI.

Una seconda possibilità – benché più lunga e impegnativa – consisterebbe nell'emanazione di una disciplina degli sport virtuali sulla falsariga della riforma del lavoro sportivo.

In entrambe le ipotesi, però, il risultato conseguito non sarebbe del tutto soddisfacente, in quanto – pur sviluppandosi su distinti binari e con velocità diverse – entrambe partirebbero da un presupposto non pienamente convincente e condivisibile, ossia la sovrapponibilità tra i due settori.

Per quanto sussistano affinità e possa risultare utile attingere all'esperienza pluridecennale della regolamentazione sportiva, la disciplina e le tutele specifiche degli *e-Sports* non possono prescindere dalle loro caratteristiche e, in particolar modo, dal fattore tecnologico che li connota, con tutte le implicazioni del caso. È la digitalizzazione il punto focale attorno al quale dovrebbero snodarsi le previsioni e le garanzie giuslavoristiche per l'attività e-sportiva.

D'altronde, l'applicazione agli *e-Sports* delle tradizionali categorie sportive del professionismo e del dilettantismo[117] – con tutti i conseguenti adempimenti – rischierebbe di tradursi in un orpello superfluo e anacronistico e non risponderebbe alle reali esigenze di tutela dell'integrità psicofisica[118] dei soggetti coinvolti e di valorizzazione della loro professionalità. Ad esempio, l'assenza non soltanto di riferimenti normativi, ma anche della contrattazione collettiva e della presenza sindacale[119] nel settore e-sportivo è una delle cause della non adeguata remunerazione a livello nazionale, che può ripercuotersi sulla scarsa professionalizzazione dei *pro-players* italiani[120]. Talvolta le stesse «modalità di remunerazione dell'attività appaiono non codificate e variabili»[121], oscillando tra chi rinviene la principale fonte di reddito nel montepremi delle competizioni virtuali e coloro che vengono ingaggiati da squadre e-sportive percependo un compenso fisso, talora dall'importo irrisorio, con grave lesione del diritto costituzionale alla "giusta"

---

116 V. Protocollo CONI-Comitato Promotore E-Sports Italia del gennaio 2022.

117 In via di graduale superamento anche nel settore sportivo, come lascia presagire il d. lgs. 36/2021.

118 V. par. 4.3.

119 A differenza del settore sportivo, in cui, seppure soltanto negli ultimi anni, si è sviluppata l'attività sindacale: al riguardo, v. CCNL sottoscritto il 12 gennaio 2024. V. anche i riferimenti presenti nel c. 3 dell'art. 25 d. lgs. 36/2021 agli «accordi collettivi» e alle «organizzazioni comparativamente più rappresentative, sul piano nazionale, delle categorie di lavoratori sportivi interessate».

120 Sul punto v. OIES, *White Paper Esports,* cit.*,* 55.

121 E. Rocchini, *Esports e diritto del lavoro: osservazioni sul rapporto di lavoro dei proPlayers*, in *Massimario di Giurisprudenza del Lavoro*, 1, 2024, 121.

retribuzione[122].

Un'altra sfida impegnativa è l'inclusione delle donne negli *e-Sports* a livello professionale[123]. Anche se i dati più recenti appaiono rassicuranti[124], al momento le pari opportunità nel settore non sono affatto garantite: numerosi sono gli ostacoli e le resistenze all'ingaggio di giocatrici e allenatrici nelle squadre virtuali e, anche laddove ciò avvenga, si registra un significativo divario retributivo tra uomo e donna[125], in violazione di quanto sancito dal primo comma dell'art. 37 Cost.

Infine, la disciplina *ad hoc* degli *e-Sports* dovrebbe prendere in esame anche la miriade di figure professionali che ruotano intorno al settore e-sportivo e all'attività del *pro-player*, come, ad esempio, lo *streamer*[126], il *caster*[127] e il *cosplayer*[128]. Per quanto non appaiano assimilabili ai profili professionali elencati nell'art. 25 d. lgs. n. 36/2021 in riferimento al lavoratore sportivo, sono comunque meritevoli delle tutele previste dall'art. 35 Cost. per «il lavoro in tutte le sue forme ed applicazioni».

Alla luce di ciò, l'emanazione di un provvedimento normativo sul lavoro e-sportivo non è prevedibile in tempi brevi, anche perché i disegni e le proposte di legge finora presentati prendono in esame soltanto alcuni aspetti della vasta e variegata materia e non risultano esaustivi. Un'accurata regolamentazione del lavoro e-sportivo nel suo complesso richiede non solo tempo e competenze, ma anche grande attenzione alle criticità e alla gestione dei delicati equilibri presenti in un settore nuovo e in continua evoluzione, confermando così che gli *e-Sports* non sono (soltanto) un gioco.

[122] Il richiamo è all'art. 36, c. 1, Cost.

[123] Sul punto v. M.C. Vitucci, *Genere e e-sports: dalla discriminazione all'inclusività*, in G. Bevilacqua - A. Lepore, *E-sports, sicurezza e diritti umani,* cit., 11.

[124] Secondo l'*Italian Interactive Digital Entertainment Association*, nel 2022 ben il 42% dei 14,2 milioni di videogiocatori in Italia è composto da donne.

[125] V. F.M.R. Livelli, *eSport: quanto è diffuso il gender gap e come superarlo*, in *Agenda Digitale*, 27 gennaio 2022.

[126] È il soggetto che gestisce un canale su una piattaforma di *streaming* (ad es., Twitch.tv), dal quale trasmette video in diretta, relativi all'ambito dei videogiochi e delle competizioni videoludiche, intrattenendo gli spettatori (attraverso un microfono e una videocamera) e interagendo con loro tramite una chat apposita.

[127] È una sorta di commentatore delle partite e-sportive, al quale, però, a differenza dei cronisti sportivi, non è al momento riconosciuta la possibilità di chiedere il tesserino come giornalista pubblicista: v. OIES, *White Paper Esports,* cit., 69 ss.

[128] Il *cosplayer* interpreta i personaggi dei videogiochi indossando appositi costumi e interagendo con il pubblico delle competizioni e-sportive per suscitare un maggiore coinvolgimento: v. OIES, *White Paper Esports,* cit., 72 ss.

Toward ne(X)t neutrality. A re-thinking of the EU Open Internet Regulation*

Antonio Manganelli

Abstract

This paper focuses on net neutrality regulation, which in the EU is considered and designed as a legislation mainly aimed to protect end-users' interest, within the composite electronic communications' regulatory framework.
For this reason, the current EU Open Internet Regulation has been developed without a sound consideration of its economic impact on markets, in terms of static and dynamic efficiency, which has been identified as one of the main problems regarding the implementation of Net Neutrality rules in Europe, especially in light of new technologies development. This pitfall has been intensified by the significant technological and market changes happened in the last few years within the "extended digital ecosystem" where a much wider set of players interplay. These evolutions transformed market positions of the largest Content and Application Providers (CAPs) both in terms of countervailing power and their ability to influence end-users' internet experience. In this context, the paper advocates for a ne(x)t neutrality approach, embracing a "proportionality" principle as well as having a systemic perspective and thus reframing the existing asymmetric approach vis à vis the different actors in the digital ecosystem.
A first step in this direction would be to update and clarify at the EU level the Open Internet Regulation's provisions, by embracing an interpretation that takes into account technology and market evolution. A second step would be grounded on a more radical rethinking, by allowing more flexibility and freedom for ISPs to implement a quality differentiation, as for premium quality services, as well as for zero-rating offers, both as 'class-based offers' and 'content-specific retail offers', yet only when it is the end-user choosing for such a differentiation. This could be done by introducing an 'application-agnostic anchor product' for IAS with a minimum QoS that all users are enabled to choose. This consumer-empowering approach to net neutrality could strike an effective regulatory balance by guaranteeing a freedom of choice, on one side, yet without over-restricting the economic and commercial freedom of companies, on the other side.

Table of contents

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

Keywords

net neutrality – open internet – competition – digital infrastructures – regulation

1. Introduction: rationale(s) of the net neutrality debate(s)

Telecommunications operators (shortened often here as telcos) traditionally provide services enabling «direct interpersonal and interactive exchange of information via electronic communications networks involving a finite number of persons». This is the current definition of an 'interpersonal communications service', under European Electronic Communications Code (EECC). [1] When it comes to the Internet, telcos had and still have a clear role, i.e., to provide connectivity.[2] Therefore, besides providing 'interpersonal communication services', telcos enable the distribution of digital services, contents, and applications to end-users over their (high-speed)[3] telecommunications infrastructures by providing end-users with internet access services (IAS):[4] they therefore work as Internet Service Providers (ISPs). Those contents, information services and applications (also called information society services, ISS[5]) are usually[6]

[1] Art.2 EECC: directive (EU) 2018/1972. Overall, electronic communications services comprise (i) internet access service; (ii) interpersonal communications services (iii) services consisting wholly or mainly in the conveyance of signals.

[2] Electronic communications services are disciplined by the European Electronic Communications Code (EECC: directive (EU) 2018/1972) and comprise (i) "internet access service"; (ii) interpersonal communications services (iii) services consisting wholly or mainly in the conveyance of signals.

[3] Within the 2018 EECC, investment promotion toward very high-capacity networks has become a new independent general objective of the European strategy. Accordingly, National Regulatory Authorities are mandated to «promote connectivity and access to, and take-up of, very high-capacity networks [VHCN], including fixed, mobile and wireless networks, by all citizens and businesses of the Union». See A. Manganelli-A. Nicita, *The Governance of Telecom Markets*, London, 2020.

[4] An "internet access service" is a service that provides access to the Internet and, thereby, connectivity to virtually all end points of the Internet, irrespective of the network technology and terminal equipment used. Art. 2 EECC.

[5] An information society service is generally defined as «any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services». Those can be video streaming services, search engines, email services and so on. These have been originally disciplined by the E-Commerce Directive (directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market) as amended by the Digital Service Act (DSA, regulation (EU) 2022/2065 on a Single Market For Digital Services) and recently by the Digital Markets Act (DMA, regulation (EU) 2022/1925 on contestable and fair markets in the digital sector).

[6] Actually, the digitalisation has implied a process of multimedia convergence (i.e., a range of different

not provided by ISPs and end-users needs to buy them from other players within the internet ecosystem, i.e., from content and applications providers (CAPs). Therefore, IAS and ISS work as complements to satisfy the needs of an internet end-user.

In the internet landscape, there were (and still partially there is) an asymmetry in the complementarity relationship between the providers of those services and that asymmetry was one of both technical and economic nature. Indeed, ISPs have the material and technical capacity to manage content data traffic (i.e., throttling, prioritising or blocking data packages), consequently, affecting the service quality (or even the availability) of content and application for end-users. On the contrary, CAPs didn't play any role in the distribution of their content. Moreover, under an economic perspective, depending on their scale and the competitive environment, ISPs can be bottlenecks for CAPs to reach end-users and, thus, in a situation where CAPs had no countervailing power, ISPs could exert market power vis à vis both end-users and CAPs.

The network neutrality debate originated in this very context, and its core issue was to grant that «all data packets on the Internet should be treated equally»,[7] therefore framing the internet traffic on an inherent "best-effort" approach. Afterwards, the net neutrality concepts and debates took on many different hues and forms depending on the market and policy context. Anyhow, its consolidated basic definition still mainly concerns the prohibition of traffic prioritisation ("fast lane" versus "dirty roads" or, in other words, "managed services" versus "best effort" ones), with or without compensation for these differentiations.[8]

Indeed, the "best effort" approach was a win-win strategy in a technical environment of non-time-sensitive applications, i.e., simple email exchanges and web browsing, with quite decentralised and symmetric data flows, needing low bandwidth, with very scarce risk of congestion. In that situation, traffic management and prioritisation (if any) would be likely undertaken to obtain some economic advantage rather than to aim at an efficient use of network resources.

Under an economic viewpoint, the underlying theoretical assumption was that, without any net neutrality obligations, ISPs would have set a system of data paid termination, as for voice calls,[9] and consequently exploit their market power by charging ex-

digital content and services to be transmitted on the same digital network) which has allowed telcos to provide some additional services, i.e., multi-play offers, for example Audiovisual content. Those offers including both fixed broadband and IPTV, currently represent a significant portion of total broadband subscriptions in Europe. See A. Manganelli-A. Nicita, *The governance of Telecoms markets*, cit.

[7] T. Wu, *Network Neutrality, Broadband Discrimination*, in *J. on Telecomm. & High Tech*, 2, 2003, L. 141.

[8] S. Greenstein-M. Peitz-T. Valletti, *Net Neutrality: A Fast Lane to Understanding the Trade-Offs*, in *Journal of Economic Perspectives*, 30(2), 2017, 127 ss.

[9] Telecommunication sector has been designed by regulation, *ab origine*, as an interconnected networked system, where each user can communicate with any other user, even if they subscribed to different retail (fix or mobile) service providers. This interconnected networked system, and its related services are divided into: (i) call origination and collection, (ii) call transit and (iii) call termination. If the calling party and receiving party belong to different network (off-net call), the calling user's network operator must route the signal (or data) through the called party's network operator, to 'terminate' the call. In this way, calling user's network operator interconnects with the receiving party's network, 'using' a segment of its network, the termination, to reach the receiving party. In this context, European regulators have always mandated that operators terminating a call must receive remuneration for this service. This interconnection model configures each user network as a bottleneck, as it is the only having access

cessive termination fees for CAPs. This would be implemented by threatening to put in place non-price discrimination practices, e.g., by blocking some CAPs or degrading their quality of service (QoS). This could also work as a self-preferencing strategy, should an ISP be vertically integrated and provide content or application services, thus favouring their own content provisions by vertically leveraging market power to reduce competition and exclude competing content and applications.

As for the latter, in the US, where the net neutrality debate originated, the risk of self-preferencing by vertically integrated ISPs, with anticompetitive exclusionary effects on other CAPs, was and is one of the main concerns as for the neutrality of the internet.[10] In the US dominant ISPs are vertically integrated with very large content providers (e.g. Comcast merged with NBC-Universal in 2011 and with Sky in 2018, and AT&T merged with Time Warner in 2018). Thus, ISPs in the US offer bundled communications and audio-visual managed services, directly competing with other very large CAPs. As for Europe, in some member states, triple and quadruple-play bundles offered by telcos, including digital television, started to become common, however, in the EU there is not such a widespread vertical integration between internet access providers and audio-visual content as there is in the US.[11] In addition, differently from the EU, the US Internet access market is very concentrated end-to-end.[12]

Further to rationales related to the exploiting or leveraging of market power, another important aspect of the net neutrality debate was related to the internet traditions of freedom, openness, and equality. [13] Indeed, the internet was born and developed under a sort of net neutrality "natural law" or "social contract", not imposed by regulation but resulting as a spontaneous market outcome from decentralised market interactions.[14] In the EU, the net neutrality debate has been mainly developed under this con-

to the user and thus is essential for the termination of calls to him. See A. Manganelli-A. Nicita, *The governance of Telecoms markets*, cit.

[10] As a matter of fact, the debate around the "neutrality" of networks was originated in the US debate with regard of the relationship between telecom network operator, telecom service providers, on one side, as a means of ensuring market fair competition and between service providers and end-users, on the other side, in order to guarantee end-users access to a "common carrier". Then it was extended to the relationship between internet access service providers and end-users/content providers, yet applying the same legal base: i.e., Telecommunications act 1996. See M. Orofino, *La declinazione della net-neutrality nel Regolamento europeo 2015/2120. Un primo passo per garantire un'Internet aperta?* in *Federalismi.it*, 2, 2016.

[11] The closest case in the EU was the conditioned clearing decision about the Liberty Global/Ziggo merger, for concerns about degrading rival broadcast channels.

[12] M. Cave-I. Vogelsang, *Net Neutrality: An E.U./U.S. Comparison. Competition Policy International,* 11(1), 2015, 85 ss.

[13] Among many, see D.C. Nunziato, *Virtual Freedom: Net neutrality and Free Speech in the Internet Age*, New York, 2009; L. Belli-P. De Filippi, *Net Neutrality Compendium: Human* Rights*, Free Competition and the Future of the Internet*, Cham, 2016.

[14] These visions were (and for certain aspects still is) at the base of the main cultural motivation "not to regulate the internet": a place not to be subject to "governments' rules" yet only to "its own" rules. Of course, it is not trivial who and how these endogenous rules are defined. On these aspects, see A. Manganelli, *Digital Platforms and social networks: plurality of legal orderings, media pluralism and market power,* in *Giurisprudenza costituzionale*, 2, 2023; M. Bassini, *Internet e libertà d'espressione. Prospettive costituzionali e sovranazionali,* Roma, 2019; M. Cuniberti, *Potere e libertà nella rete*, in *Rivista di diritto dei media*, 3, 2018, 39 ss.

ceptual framework, as an end-user's right to access digital services and contents in a universal, equal, and non-discriminatory manner.[15] This is why the EU Open Internet Regulation (2015, OIR)[16], described in details in the following section, did not actually modify the electronic communications' access and interconnection regulatory regime, dealing with market power and anticompetitive discriminations, but those rules regarding universal services and citizens' rights.[17]

On this basis, the EU net neutrality regime considers also some technical and efficiency needs for traffic management; nevertheless, neglects the importance of the economic interplays between ISPs and CAPs, their radical evolution, and the impact that this may have on competition dynamics (in the two markets) and ultimately on consumer welfare in the overall digital ecosystem.

This issue is at the very core of this paper, which starts from a description of the EU Open Internet regulation (section 2), then describes the ongoing technical and economic changes calling for a possible legislative review (section 3) and what kind of revisions may be sensible to consider (section 4).

Net neutrality rules have always and continuously been at the centre of policy and regulatory debates. So much so that the UK telecom and media regulator, Ofcom, has recently issued a report assessing the net neutrality regime.[18] Regardless the outcome of that analysis, which is obviously considered in the paper, it is significative that the impact assessment of net neutrality rules in the market has been one of the first post-Brexit policy action undertaken by Ofcom as soon as the EU regulation has ceased to be binding.

Furthermore, it is very recent news that an US appeals court ruled that the US Federal Communications Commission (FCC) did not have legal authority to reinstate net neutrality rules, as it was done by the FCC's 2024 Safeguarding and Securing the Open Internet Declaratory ruling and Order. Despite the clear relevance of the substantive net neutrality debate in the US, [19] it is crucial to highlight that the judicial and regulatory dynamics in the US are not automatically meaningful for the EU context. First, the main US legal/judicial disputes across the last 15 years are very specific to the US legal system. These were mainly about the FCC competence to regulate discriminatory treatments of Internet traffic (as done in 2010, 2015 and 2024[20]) primarily

[15] Nevertheless, differently from the universal service obligations concerning electronic communication services, i.e., arts. 84 and 85 EECC, the universality and non-discriminatory provision of digital contents was not based onto regulatory obligations imposed on the providers of those services, but on the network intermediaries. In other words, when it comes to online commercial content and application services, net neutrality rules in EU have been designed as Universal service obligations imposed to telcos in order to allow universal access to contents and applications and therefore the possibility for users to buy those services and for CAPs to sell their products/services.

[16] Regulation (EU) 2015/2120 laying down measures concerning open internet access.

[17] Respectively the Access directive, directive 2002/19/EC, and universal service and users' rights directive, directive 2002/22/EC, then both transfused into the European Electronic communications code, directive (EU) 2018/1972.

[18] Ofcom, Statement – *Network Neutrality Review*, 26 October 2023.

[19] Among many, due to the seminal and conflicting ideas of its authors, see, T. Wu-C. Yoo, *Keeping the Internet Neutral? Tim Wu and Christopher Yoo Debate*, in *Federal Communications Law Journal*, 2007.

[20] In a nutshell, the 2015 Order, temporarily restored by the 2024 one, established three specific

revolving around the extension of the "common carrier" status to the ISPs under the US Communications Act 1934 and Telecommunications Act 1996.[21] Second, US net neutrality has been disciplined by the FTC, where no specific rules are set by primary federal legislation, and this has been done through "regulatory policies" that are very dependent upon political dynamics: e.g., 2015/2018/2024 flip-flopping according to government turnovers.[22] This implies that those rules were scarcely based on the actual economic and technological context[23] - in contrast to this paper's objective while looking at the EU legislation.

2. Current EU regulatory approach

The EU Open Internet Regulation (OIR, enacted in 2015) grants end-users with enforceable rights to access and distribute information, contents, and services. [24] In doing so, obligations are placed on ISPs to «treat all traffic equally ... without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used».[25] However, "reasonable" day-to-day traffic management practices are allowed as long as they are (a) transparent, (b) non-discriminatory, (c) proportionate and (d) not based on any commercial considerations but on objectively different technical quality of service requirements for specific traffic categories.
As a preliminary comment, it is important to note here that the distinction between technical and commercial considerations could be inherently problematic. To simplify, when traffic management practices are necessary due to congestion phenomena (so problems of technical matter) network operators always have the alternative of improving QoS by investing and expanding the network capacity rather than engaging in traffic management. However, the decision to invest is an economic decision, which could not be profitably done without considering the overall economic context, where telcos operate.
In any case, these measures may be maintained no longer than is necessary and cannot involve deep packet inspection. Some practices are clearly considered non-reasonable,

prohibitions: (i) no-blocking, (ii) no-throttling, and (iii) no-paid-prioritization, plus (iv) a residual ban on unreasonable discrimination.

[21] In the latest judicial decision in January 2025, judges cited *Loper Bright Enterprises v. Raimondo*, i.e., the Supreme Court case that in June overturned the so-called "Chevron deference": this means courts no longer need to follow FCC's interpretation (or other federal agencies') to apply legal provisions characterised by a certain level of ambiguity. As a comment: this seems particularly appropriate in order to provide some legal certainty and stability in context where an administrative agency continuously changes its approach/interpretation. As for the debate about "common carrier", see: C. Yoo, *Is there a Role for Common Carriage in an Internet-based World?*, in *Houston Law Review*, 51, 2, 2013, 545 ss.

[22] Those are (i) 2015 Open Internet Order (based on Obama's "mandate"), (ii) 2018 Restoring Internet Freedom Order (based on Trump's "mandate", and lastly (iii) 2024 Safeguarding and Securing the Open Internet Declaratory ruling and Order (based on Biden's "mandate").

[23] See P. Damiani, *The open Internet vs. net neutrality and the free Internet*, in *Federalismi.it,* 8, 2019.

[24] Art 3(1) OIR - Safeguarding of open internet access

[25] Art 3(3) OIR.

should they «block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services». There are three general exceptions to this general rule where (i) compliance with legal obligations, (ii) network integrity and (iii) congestion management in exceptional and temporary situations are involved. The exception (iii), i.e., network congestion, is related to the fact that data traffic volumes over the network are continuously skyrocketing and networks, despite the ongoing technical improvements, may not be able to operate effectively and ensure contractual commitments for the higher quality services are met. Therefore, in certain circumstance, specifically in times of congestion, it may be necessary to apply traffic management measures to differentiate between the different tiers of service. The current guidelines do not explicitly confirm that such an approach to traffic management would be permissible, since current rules and the BEREC guidelines[26] allow ISPs to go beyond reasonable traffic management if necessary and only for as long as necessary, in order to prevent network congestion and mitigate the effects of exceptional or temporary network congestion, provided that equivalent categories of traffic are treated equally. Therefore, according to BEREC guidelines, when there is recurrent and more long-lasting network congestion, ISPs cannot apply traffic management practices but must invest to expand their network capacity.[27]

This positioning is clearly reinforcing the point made earlier about the overlap between technical and business considerations, taking an economic decision that could be disregarding all the efficiency and welfare aspects. Indeed, installing more network capacity just to handle peak load traffic leads to private costs for the ISPs as well as significant social costs.[28]

Regulation also allows for the provision of *specialised services*, deemed as those services «optimised for specific content, applications or services … where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality»[29] or, in other words, those services that need to be carried out at a specific level of quality that cannot be assured by the standard best-effort delivery. The regulation defines specific safeguards to be respected for the provision of specialised services to ensure that the open Internet is not negatively affected. Specialised services (a) can be satisfied by the network capacity residual to any IAS provided; (b)

[26] BEREC, *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules,* BoR (16) 127, and afterwards BoR (20) 112, and lately BoR (22) 81. In Italy, in order to avoid network congestion resulting from traffic peaks and a degradation of quality of service for all internet customers, the national regulatory authority AGCOM required DAZN, which broadcasts "Serie A" football matches over the internet, to provide ISPs with equipment to be integrated into their networks to handle a substantial share of the overall DAZN-originated live streaming data traffic (AGCOM decision n. 206/21/CONS). AGCOM's decision aimed to preserve network integrity and protect consumers, yet this could not be based and refer to the current net neutrality rules. In making this order AGCOM, giving an extensive interpretation of some Code provisions, considered the CDN as subject to the electronic communications code, including the general authorisation regime. Afterwards, a government's legal provision gave AGCOM's decision a more solid legal basis.

[27] BEREC 2022 NN guidelines, para. 93.

[28] For example, because more cell towers need to be installed in somebody's neighbourhood (often appealed by citizen's initiatives), higher energy consumption and more electromagnetic interference. See J. Kramer-M. Peitz, *A fresh look at zero-rating*, in *Telecommunications Policy*, 42(7), 2018, 501 ss.

[29] Art 3(5) OIR.

are not usable or offered as a replacement for IAS; (c) are not to the detriment of the availability or general quality of the IAS for end-users; and (d) are optimised for specific content, applications or services, and that optimisation is objectively necessary to meet requirements for a specific level of quality.

Furthermore, the regulation defines transparency obligations for providers of internet access services additional to those existing for electronic communication service providers.[30] In particular, contracts for internet access services must include easily accessible, accurate, meaningful and comparable information, covering (a) any traffic management measures used, and any impact on the end-user (e.g., quality of internet access, end-user privacy and personal data protection); (b) any data caps, speed and other quality of service parameters which may in practice impact internet access; (c) how any specialised services, to which the end user subscribes, might in practice affect the same end-user's internet access services; (d) the download and upload speed of internet access services (with different metrics depending on fixed or mobile network); and (e) the remedies available to the consumer in case of any regular discrepancy between the actual performance of the internet access service and the contractually agreed on one.

As for enforcement, national regulators are empowered to closely monitor market developments and assess traffic management, commercial agreements and the compliance with transparency obligations in order to ensure the availability of non-discriminatory and transparent internet access at levels of quality that reflect advances in technology. For this purpose, national regulators may impose minimum quality of service requirements on internet access providers and other appropriate measures to ensure that all end-users enjoy an open internet access service. They must report annually on their findings to the Commission and the BEREC.[31] Moreover, according to the regulation provisions, in order to enhance a consistent application of the regulation, BEREC drew up detailed guidelines, in 2016, 2020 and 2022, which national regulators must take strictly into account.[32]

As for the commercial relationship between telcos and end-users, the OIR explicitly established the freedom to conclude agreements between ISPs and end-users relating to commercial and technical conditions, as well as IAS aspects regarding price, data volumes or speed, and any commercial practices. Nevertheless, such agreements and commercial practices must not represent a limitation in the exercising of end-user rights and, consequently, circumvent provisions safeguarding open internet access.[33]

In this context, one of the main points of debate about net neutrality concerned the zero-rating, which is a commercial practice whereby an ISP does not subtract data usage associated with specific content or a class of content from a customer's data allowance.

---

[30] Art. 4 OIR

[31] Under art. 5 OIAR, NRAs have published so far three set of yearly report, which have been sent to the Commission and BEREC.

[32] BEREC, *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules*, BoR (16) 127, and afterwards BoR (20) 112, and lately BoR (22) 81.

[33] Recital 7 and art. 3(2) OIAR.

Zero rating practices are based on data cap usage commercial practices. The latter are not covered by net neutrality rules and are normally allowed as internet connectivity retail markets are not regulated. A data cap is a legitimate pricing strategy as well as a measure to somehow avoid congestion, yet also create an artificial scarcity, making different content work as substitutes for end-users and, thus, intensifying the competition among content providers.[34] As for the general case, in this context of data cap commercial offers, zero-rating represents a contingent competitive concern where a vertically integrated ISP would exempt its own traffic, in order to favour its content. A connected yet different issue is that of zero-rating agreements with a third-party CAP. In this situation, data caps could induce CAPs to compete for the "fast/zero-rated lane". In this competition, larger CAPs would likely to prevail, also because of their must-have contents, usually in exchange of prioritisation or data-free payment. So, by prohibiting zero rating, policy makers want to avoid large CAPs locking-in users. Yet again an obligation aimed to impede large CAPs exertion of market power is however imposed on telcos.

Initially this practice has been considered compatible, on a case-by-case basis, with net neutrality regulation (2016 and 2020 BEREC net neutrality guidelines). Under those BEREC guidelines only some practices were clearly prohibited – for example, those where all applications are blocked or slowed down once the data cap is reached, except for the zero-rated application(s). Other practices were considered in need of a specific operational assessment to be carried out by NRAs using the following criteria: (a) whether the practices circumvent the general aims of the regulation (to «safeguard equal and non-discriminatory treatment of traffic» and to «guarantee the continued functioning of the internet ecosystem as an engine of innovation»); (b) the market positions of the ISPs and CAPs involved; (c) any distorting effects on end-user choice, both for applications and CAPs; and d) the scale of the practice and the existence of alternatives.

In 2021, the Court of Justice of the European Union (CJEU) issued few rulings that found zero-rating offers to be unavoidably in breach of the requirement of equal treatment of traffic in Article 3(3).[35] The Court based its decision in part because these programs were based on commercial considerations rather than objectively different technical differences for specific categories of traffic. Subsequently, in June 2022, BEREC revised its Guidelines to reflect these rulings.

[34] Economides N, Hermalin E (2015) The Strategic Use of Download Limits by a Monopoly Platform. RAND Journal of Economics, 46(2), 297–327.

[35] ECJ, C-807/18 and C-39/19, *Telenor Magyarország* (2020), § 52; C-854/19, *Vodafone* (roaming) (2021), § 28; C-5/20, *Vodafone* (tethering) (2021), § 24; and C-34/20, *Deutsche Telekom* (throttling) (2021), §. 52. See G. D'Ippolito-M. Monti, *Net neutrality e "tariffe zero": la convergenza delle esigenze democratiche e di mercato*, in *Rivista di diritto dei media*, 2, 2021, 256 ss.; F. Donati, *Net Neutrality e zero rating nel nuovo assetto delle comunicazioni elettroniche*, in T.E. Frosini-O. Pollicino-E. Apa-M. Bassini (a cura di), *Diritti e libertà in Internet,* Milano, 2017, 185 ss.

3. Why a revision of the Open Internet Regulation could be considered

The EU commission in its recent report on the net neutrality rules enforcement has highlighted that OIR «was deliberately conceived as a principle-based set of rules that could be applied to the foreseeable development of new technologies».[36] Therefore, in principle, this would allow an evolutive interpretation that could fit any technical and market transformations; furthermore, to reduce the ex-ante uncertainty (deriving from the utilisation of general principles) and not to inhibit innovation, BEREC has been empowered to provided guidelines.[37] Nonetheless, the EU commission implementation report signalled that: «Greater legal certainty could therefore be beneficial to both innovators and consumers in the future».[38]

As mentioned, the rules currently in force allow for ISPs and CAPs to offer 'specialised services' and this seems to be the crucial point in order to understand whether current rules inhibit telecom industry to fully deploy new technologies capabilities and consequently affect end-users' choice and welfare. In this regard, two main points of concerns rely upon (i) legal uncertainty created by the current case-by-case approach embraced by the BEREC guidelines, and (ii) possible restrictive interpretation of the criteria concerning the detriment for the general quality of the IAS for end-users, for which there is no clear definition.

In addition, guidelines cannot modify the fundamental approach of the regulation, tending to overlook the economic interplays between ISPs and CAPs and consequently at those crucial technological and market changes having took place in last years.

Another assessment, with a wider and unconstrained perspective, has been done by the UK regulator Ofcom, which was considering for revision the overall net neutrality regime in order to clarify the applicable rules and relax some constraints for ISP activity. At the basis of Ofcom's analysis stands the fact that the current rules «may be restricting their ability to innovate, develop new services and manage their networks. This could lead to poor consumer outcomes, including higher costs, or consumers not benefiting from new services as quickly as they should, or at all. These potential downsides might become more pronounced in the future, as people's use of online services expands, traffic increases, and more demands are placed on networks».[39] Furthermore, within its market assessment, Ofcom noted that, within the current EU approach, «net neutrality rules limit the actions ISPs can take, but do not restrict other parties in the value chain. Since the rules were put in place, players with strong market positions have developed throughout the internet value chain and are not constrained

[36] European Commission, *Report on the implementation of the open internet access provisions of Regulation (EU) 2015/2120* – COM (2023) 233 final

[37] BEREC, *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules*, cit.

[38] European Commission, *Report on the implementation of the open internet access provisions of Regulation (EU) 2015/2120*, cit.

[39] Ofcom, *Net Neutrality review,* cit.

in the same way as ISPs by the net neutrality rules».[40]
Therefore, it seems crucial to assess technological, market and business models changes that occurred in the sector that may undermine assumptions underlying the current net neutrality rules.

3.1. Technological changes weakening the OIR's assumptions

As anticipated the main rhetoric about net neutrality is associated with individual rights based on a conceptualisation of the internet ecosystem as composed of decentralised and atomistic users that symmetrically exchange traffic, information and content.
Nowadays, this vision of the web as a place where individuals and small enterprises interact in a decentralised way is no longer true due to the radical transformations the internet and the web have undergone. These transformations have involved the internet structure, shifting from a decentralised setting toward a centralised one, where extremely large digital players have enormous scale and are active in many digital service and products markets, including private electronic communications networks. Consequently, these transformations also profoundly affected the data traffic, tendentially shifting from symmetric flow to heavily asymmetric.
Indeed, today, the great majority of internet data packets are related to contents and services which are mostly unidirectional - from content providers to users - and a drastic increase in traffic volume, with low latency requirement is happening and is likely to continue in the future.[41] These shifts imply that, on one side, traffic management practices could have a technical motivation related to the efficient usage of the network (and this element is crucial for 5G networks) and, on the other side, that traffic flows are usually asymmetric and related to the activity of few market actors[42] – which are anyway provided by the the OIR with the same kind of protective relationship vis à vis ISPs reserved to an individual end-users.
As for the first point, progressive deployments of 5G networks have been bringing increased opportunities to provide different services and innovations strictly interlinked with applications and use cases that differ significantly in their network requirements. Indeed, 5G mobile broadband is mostly about differentiation of quality of service (QoS) and quality of experience (QoE), especially looking at "network slicing".[43] In

[40] *Ibidem.*

[41] For detailed general reference, see Analysys Mason, *The impact of tech companies' network investment on the economics of broadband ISPs*, 2022, October 2022, 23; TeleGeography, *The State of the Network*, 2023 Edition, 10; Sandvine, *Global Internet Phenomena Report,* 2023, 7; *Ericsson Mobility Report*, 2022, 18; Sandvine, *Global Internet Phenomena Report*, 2023, 22; Arthur D. Little, *The Evolution of Data Growth in Europe,* Report 2023, 18.

[42] In 2022, almost half of data traffic (precisely 47%) has been generated by only 6 big digital players (i.e., Netflix, Google, Facebook, Amazon, Apple and Microsoft). See, Sandvine, *Global Internet Phenomena Report*, cit.

[43] As part of this new business model, 5G is also being deployed around a new technological approach

principle, this is in contrast to the "best-effort" approach underlying the original net neutrality concept, which could not embrace QoS and QoE differentiation, as efficient practices to be allowed and encouraged as much as possible.

It is true, as mentioned, the rules currently in force allow for ISPs and CAPs to offer 'specialised services'; however, possible interpretations of the EU's OIR might be inconsistent with network slicingand other innovative approach to 5G. [44]

In addition, other technical issues may drastically change the assumptions underlying the current net neutrality rules in the EU. Nowadays it seems that not solely ISPs can influence the traffic flow. In this regard, an open question originating from the technological development in mobile 5G communications concerns whether other subjects, e.g., operating system providers (i.e., mainly Google Android and Apple iOS), could somehow control the different network's slices.[45] Indeed, to correctly identify and transmit traffic according to the specifications of the slices, an interaction between the network and the device is necessary. The OS players cover a crucial role, as the routing of the application to the slice depends on the OS of the end-user, and in some situations the operator must apply a configuration designed by the OS provider to connect the application and the slice. This being said, given the concentration of the consumer market for device OS,[46] there is a risk that major OS providers are in a position *de facto* to impose standardisation to the slicing identification mechanism and that, as an effect, operators may lose part of the control over which traffic corresponds to each slice.

In the same fashion, content delivery networks (CDNs)[47] enable to some extent service differentiation by managing traffic via private networks and ensure content is

known as network slicing, which enables a network to be divided into multiple subnetworks (called slices) that different users can use simultaneously in much the same manner that cloud computing allows multiple virtual computers to share the same servers. Network slicing creates several benefits. Resource sharing allows more efficient utilization than would occur if each resource were dedicated to a single user or use case. Sharing efficiency is particularly important for technologies that, like 5G, depend on lower-powered microcells that necessarily serve fewer customers. In addition, individual slices can each be tailored to provide different levels of quality of service (QoS) to each application.

44 C. Yoo, *Network slicing and net neutrality*, in *Telecommunications Policy*, 48(2), 2024.

45 BEREC, *Report on the entry of large content and application providers into the markets for electronic communications networks and services,* 2024 - BoR (24) 139.

46 As stated in BEREC, *Report on the Internet Ecosystem,* 2022 - BoR (22) 167, the mobile OS market in Europe is mainly split between Android (63.6% market share by 2022) and iOS (35.7%). Apple iOS and Google Android respectively define the two main mobile ecosystems and have been recently qualified as gatekeepers under the DMA. Indeed, despite a complex and layered structure consisting of devices, operating systems, and applications, mobile ecosystems are currently an oligopolistic market where two players (i.e., Apple and Google) own a gatekeeping position, being responsible for the leading mobile operating systems (iOS and Android), app stores (App Store and Google Play), and web browsers (Safari and Chrome). Because of such a strategic market status and their vertically integrated value chain, Apple and Google control access to mobile ecosystems, setting rules for (end and business) users, and compete with business users operating on their platforms.

47 A CDN is a network optimised for the distribution of digital content, which therefore increase the performance of the internet (access) network. CAPs are the main customers of a commercial CDN provider (deployed by a third party, neither an ISP nor a CAP). However, in the last few years, the largest CAPs have been investing heavily in their own CDN infrastructure (in-house CDN). In addition to in-house CDNs, large CAPs, such as Amazon, Alibaba, Google, and Microsoft are also commercially operating CDNs to support services that are used by their cloud customers.

hosted as close to the end-user as possible to guarantee certain quality levels.[48] From an user experience perspective, these and other mechanisms can act as 'technological substitutes' for network management by ISPs, ensuring higher quality of experience perceived by the end-user.[49] The fact that large CAPs 'buy' services from a commercial CDN or 'make' that service, by vertically integrating, can be seen under an economic perspective as a form of 'paid prioritization' although traffic is not prioritized in the network layer by ISPs, and thus it is not subject to OIR.[50]

In this regard, the recent Commission's White paper on digital infrastructure focuses on the fact that the current digital ecosystem is the ongoing results of extensions and overlapping of previously neatly separated value chains: «this new model of network and service provision relies not only on traditional electronic communications equipment, network and service providers but also on a complex ecosystem of cloud, edge, content, software and component suppliers, amongst others. The traditional boundaries between these various actors are increasingly blurred …»[51]

Therefore, if ISPs are no longer the only type of market players that could influence end-users' internet experience, growing significance should be attached in what other players can do in the extended value chain. This is not trivial, particularly considering, that most of those players (as the OS or integrated subject with in-house CDNs), are considered CAPs under the EU open internet regulation.

3.2. Market changes undercutting OIR's assumptions

One of the most important shifts in the internet landscape, as anticipated, revolves around the centralisation of the economic transactions on the internet/digital ecosystem. Indeed, digital markets and services are highly concentrated, and few large CAPs have significant and entrenched market power. Those CAPs have humongous scale, wide scope of services provided (enveloping end-users) and very strong network effects (both direct and indirect) and provide "must-have" contents and applications to end-users, on one side of the market, and business-users, on the other side of the market.[52] Moreover, before the recent enactment of the Digital Markets Act (DMA) and Digital Service Act (DSA), [53] very large Online Platforms/gatekeepers had been

[48] V. Stocker-G. Smaragdakis-W. Lehr-S. Bauer, *The Growing Complexity of Content Delivery Networks: Challenges and Implications for the Internet Ecosystem,* in *Telecommunications Policy*, 41(10), 2017, 1003 ss. However, on-net CDNs allow to reduce cooperatively capacity costs for ISPs by locating content closer to end-users.

[49] W. Briglauer, *Efficiency and Effectiveness of Net Neutrality Rules in the Mobile Sector: Relevant Developments and State of the Empirical Literature*, 2024, in *wu.ac.at*.

[50] T. Garrett-L.E. Setenareski-L.M. Peres-L.C.E. Bona-E.P. Duarte, *A survey of network neutrality regulations worldwide*, in *Computer Law & Security Review*, 44, 2022.

[51] European Commission, *White paper on How to master Europe's digital infrastructure needs?,* 2024, COM(2024) 81 final

[52] Often, very large CAPs are online platform structured as two (or multi) sided markets, thus intermediating between end users and business users. See A. Manganelli-A. Nicita, *Regulating digital markets*, cit.

[53] As well known, a large number of very important pieces of legislation have been adopted by EU

subject to a light-handed regulation.

Therefore, in such a situation, notwithstanding ISPs' "termination bottleneck", such very large CAPs have a strong countervailing bargaining power vis à vis ISPs that implies a strong constraint of ISPs market power and their ability to exploit it.[54] Actually, considering the fact that some of the largest CAPs are gatekeepers, i.e., a gateway for business to reach end-users, ISPs could actually be in a bargaining disadvantage.

Here, an important asymmetry in the net neutrality approach can be described when there are dominant CAPs with must-have contents: net neutrality prohibitions are one-way directional, i.e., put obligations upon ISPs not to discriminate among CAPs traffic, whereas there are, in principle, no limitations for CAPs should they want to discriminate among ISPs. Although it could be assumed that CAPs have no incentives for discrimination, at the moment, in a perspective (not so far) scenario they could have[55] , namely in situations (partially already in place) of (i) extension of the value chain, (ii) entry and vertical integration of large CAPs into the markets for electronic communications and (iii) progressive transformation of interactions between CAPs and ISPs in this extended ecosystem, from complements to substitutes.[56]

To be sure, an asymmetric bargaining power do not represent *per se* a market failure and, in principle, do not require any specific regulatory intervention. However, the point here is not having an additional regulatory intervention, rather modifying the existing one. As a matter of fact, what could be seen as a market failure is the 'market incompleteness', mainly caused by the current regulatory approach, which does not allow certain market transactions between ISPs and CAPs to take place (transactions

legislator, in order to tackle contestability, transparency and fairness issues in digital markets, *in primis*, Digital Markets Act (DMA) and Digital Services Act (DSA). The recent approval of DMA and DSA has introduced a more stringent set of rules for very large online platforms (as defined by DSA) and gatekeepers (as defined by the DMA), however neither of these new regulatory regimes is really tackling the significant concentration of market power. See A. Manganelli, *The interplay between telecommunications operators and digital platforms in an evolving digital ecosystem*, in *Journal of Law, Market & Innovation*, 3(2), 2024, 113 ss.

[54] In this regard, it is very interesting the litigation of Deutsche Telekom v. Meta: the German ISP and the global CAP had a contractual agreement under which DT would deliver data traffic between Meta and its end-users via direct connections for a fee ("paid peering"). During the coronavirus crisis, Meta stopped making these payments, then Deutsche Telekom filed a lawsuit against this and was upheld by the Cologne Regional Court (case 33 O 178/23). In that context, Meta charged DT for exploiting its dominant position on the IAS by charging excessive fees. The court, however, did not find that Deutsche Telekom abused its market power by charging excessive fees for the handling of data traffic on its internet backbone and ordered Meta to honour its contract on paid peering fees. The court in Cologne considered the different bargaining power of the two companies on the market for IP data transit services, Meta's dominant position in social networks, and its designation by the Bundeskartellamt (decision B 6 – 27/21) as having «paramount significance for competition across markets» pursuant to Section 19a(1) German Competition Act (GWB).

[55] For example, considering a scenario where CAPs start to provide IAS (e.g., Amazon via its low orbit satellite, Project Kuiper), under a vertical integration setting CAPs with must-have contents may have economic incentives to discriminate between IAS, either for extracting some rents (paying for the content and services) or for favouring its own IAS. Of course, if CAPS are dominant player, provisions related to abuse of dominant position put some constraints against an abusive vertical leveraging of market power.

[56] See, BEREC, *Report on the entry of large content and application providers into the markets for electronic communications networks and services* - BoR (24) 139.

that may well be efficiency and welfare enhancing). Therefore, a possible intervention should be aimed to correct a possible "regulatory failure". Indeed, these impediments are not only depending on market dynamics but are also based on legal provisions, since net neutrality prohibitions have augmented the existing asymmetry.

In addition, in most circumstances ISPs are "competitive bottlenecks"[57] meaning that ISPs receive competitive constraints not only from very large CAPs but also from other ISPs. Indeed, competition between ISPs for end-users, mainly in the mobile internet connection market, yet also for the fixed lines, has strongly developed in the telecom markets, due to decades of pro-competitive access regulation.[58] Consequently, any activity by ISPs blocking or degrading the quality of must-have contents/applications to their subscribers, or even of other contents/applications, would be 'sanctioned' by (empowered) end-users by switching to another ISP.[59] Just think of an ISP blocking or degrading the QoS of Google search, Youtube, Netflix, or Facebook for its users; its customer base would shrink very quickly.

As mentioned, telecommunications operators have been subject for more than two decades to pro-competitive access regulation on the supply side,[60] which has increase competition on fixed and mobile IAS markets: this implies that currently ISPs would have no incentive to put in place traffic management to deteriorate the end-users' experience and restrict their choice;

Instead, the regulatory philosophy underlying the OIR is one of definition of a minimum quality, which is a typical quality regulation in a monopolistic market, aimed to strictly protect end-users having no alternative choices but to be subject to a degradation of quality, as if decades of pro-competitive regulation haven't had any effect in the electronic communications market. Indeed, as described, NRAs can impose minimum quality of service requirements on internet access providers to ensure that all end-users enjoy an open internet access service. On the contrary, it would be effective toby properly empower and inform consumers and enable them to react and sanction quality variation for their services. Consequently, also moving away from a commoditisation of the industry, where the current regulatory approach has pushed it for the last years.

Indeed, thinking "out of the (regulatory) box", if one frames the net neutrality concepts and dynamics, transferring telcos' intermediary function into the digital platforms' intermediation, the asymmetric treatment emerges again: digital platforms, for example search engines or social networks, can prioritise contents that pay for a "fast

[57] This concept has been profoundly described by M. Armstrong, *The theory of access pricing in Telecommunications*, in M. Cave et al. (eds.), *Handbook of Telecommunications Economics*, Leeds, 2002.

[58] In the Electronic communications sector, downstream competition in the market for end-user services and the promotion of a level playing field is achieved by introducing asymmetric regulation, i.e. special obligations imposed only on the incumbent network operator to counterbalance its market power and competitive advantage. In the first instance, this is the obligation imposed on the former monopolist to give new entrants access to its network under price and quality conditions set by the regulator. Arts. 69 – 74 EECC

[59] M. Cave-I. Vogelsang, *Net Neutrality,* cit.; regarding any possible coordination in this respect there are competition law instruments in place.

[60] Along with a strict enforcement of merger regulation. Impeding any consolidation.

lane", i.e., sponsored contents. The digital regulations focus on transparency and users' awareness, whereas paid prioritisation is not excluded, as an essential part of those platforms' business models. [61] Notwithstanding, as anticipated, OIR prohibits to ISPs any commercial discrimination of traffic, even if the end-users would ask for it.
That's true that digital platforms are not considered network infrastructures, yet, on one side, they are using extensively private network infrastructures (or even public one, e.g., NIICS, and low orbit satellites), and on the other side, traditional infrastructure networks have undergone a path of extensive network functions virtualization.[62] It is evident that differences are shrinking.
These cases exemplify that current rules have no systemic approach for net neutrality policy and target only one part of the extended value chain that characterised the current digital ecosystem, where a much wider set of players interplay. Indeed, as expressed in the EU Commission white paper: «yesterday's separation between 'traditional' electronic communications networks/service providers and cloud or other digital service providers will tomorrow be superseded by a complex converged ecosystem. These developments raise the question whether the players in such converged ecosystem should not fall under equivalent rules applicable to all and whether the demand side (i.e. end-users and in particular consumers) should not benefit from equivalent rights».[63]

3.3. Net Neutrality when CAP's services are increasingly substitutes

This asymmetric approach creates a regulatory fragmentation which may be unfit for the current converged ecosystem. This fragmentation can be also explained with the existing (yet evolving) regulatory distinction of services: (a) electronic communications disciplined by the EECC, (ii) audio-visual media content, regulated by the Au-

[61] As far as any alteration of the "organic" ranking is transparent for end-users [art. 3(7a) Omnibus Directive; art. 5(3) "Ranking" and art. 7 "Differentiated treatment" of the P2B Regulation; art. 26 "Advertising on online platforms" DSA]. and do not favour a dominant platform's own-content vis a vis third-party one (self-preferencing) [art. 6(5) DMA]. Platform to Business (P2B) regulation: regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services; and the Omnibus Directive: directive (EU) 2019/2161 as regards the better enforcement and modernisation of Union consumer protection rules

[62] Virtualization allows network functions and resources to be delivered independently from hardware as virtual networks. Network Function Virtualization can be shared in the physical network by a number of services. Therefore, network functions are no longer physically located. Moreover, virtualization of core network functions allows operators to manage them in the cloud, using either dedicated SDN Telco Cloud infrastructure (which enables the functions of a network to be controlled by software) or virtual private networks on public clouds. Plum Consulting, *BEREC external study on the trends and cloudification, virtualization, and softwarization in telecommunications*, 2023 - BoR (23) 208.

[63] European Commission, White Paper, 2024.

dio-visual Media Directive (AVMS) [64] and (iii) information society services (ISS), which is now proving progressively inadequate as it frames competing (or anyway interplaying) services into completely different and separate regulatory regimes.

CAPs usually provide service (b) and (c), however, as seen, they are increasingly providing also electronic communications services and (using private) network. In this context, this asymmetric treatment is even more striking when referred to CAPs' services that do not work as complements vis à vis Telcom traditional communications services but are substitutes.

As a matter of fact, one of the first "extension" of CAPs within the traditional telecom value chain was related to VOIP communications services, which was one (or the only) economic triggers in EU for development of Net Neutrality rules in order to avoid the possible throttling/blocking practices by telcos of interpersonal communications VOIP services (i.e., Skype). Indeed, IP interpersonal communication services and IAS are in a vertical relationship and upstream discriminations could have been aimed to favour Telcos' own interpersonal communication services (which have been always provided).

However, the paramount difference is that in this case the possible discrimination rationale is not based on the provision of contents and applications by telcos, but on the fact that a content/application 'became' an electronic communication service, as recognised later by the current regulatory framework, defining the Number-independent Interpersonal Communication Services (NIICS).[65]

This approach allowed CAPs to enter the ECS market and offer competing ECS services, being subject to a much lighter regulatory regime, whilst being protected under the OIR, as a (business) user of internet access services, thus working as a complementor. The asymmetry here is evident if one considers that under an economic perspective, all types of different upstream and downstream electronic communications services are always in a complementarity relationship, also those provided by an access-seeker and an internet access services provider. In this situation, the EECC framework imposes access and non-discrimination obligations yet implying a remuneration for the access to the public network (of course, varying it according to the level and type of access to the network).

So, under an economic perspective, it is unclear why an extension of the value chain

[64] Directive (EU) 2018/1808. An audio-visual media service (AVMS) has the principal purpose to provide programmes, under an editorial responsibility of a media service provider to the general public, in order to inform, entertain or educate, by means of electronic communications networks. An AVMS could be either (a) a television broadcast. i.e., for simultaneous viewing of programmes on the basis of a programme schedule (linear AVMS) or (b) an on-demand AVMS, for the viewing of programmes at the moment chosen by the user and at his/her individual request on the basis of a catalogue of programmes selected by the media service provider (non-linear). A video-sharing platform service has the principal purpose to provide programme or user-generated by means of electronic communications, for which the platform does not have editorial responsibility.

[65] EECC distinguishes the interpersonal communication services (ICS) into two sub-categories: (a) number-based ICS services, corresponding to the traditional fixed and mobile voice services, in which the service is connected with numbers in numbering plans , assigned by public authorities for the routing of traffic, and not only as a user identification, and (b) the ICS services independent of the number, provided by digital platforms (e.g., Skype, WhatsApp, Facebook messenger) where the number is only the user's identification and not assigned and used for routing operations.

should imply such a substantial regulatory asymmetry, especially when dealing with electronic communications services. A net-neutrality-type of rule could thus also be (better and more consistently) framed under an access regulation viewpoint, prohibiting, as it is the case under EECC rules, upstream operators with significant market power (SMP) /bottleneck holders to discriminate an access seeker *vis a vis* its own downstream services. Of course, at this aim, NIICS providers would be necessarily subject to the EECC access and entry regulation.[66]

Should it be the case, it was also suggested to define data transmission and termination as relevant markets with a SMP identification and cost-oriented price obligations as remedies. [67] Indeed, a direct restraint on ISP market power, taking into account the two sides of the access market, would represent a less distortive solution and be more consistent with the overall regulatory framework than any net neutrality measure. For example, Net Neutrality as a zero-pricing rule can be considered a constraint on the business model of the ISP, as two-sided platform (intermediating between CAPs and end-users), forcing it to adopt a one-sided business model (i.e. charging only users and not CAPs.)

At the end, the current approach seems to represent a weakness of the current regulatory framework, deriving from the mere juxtaposition of uncoordinated pieces of legislation - that should be instead seen now as a part of a convergent extended framework for the digital ecosystem.

4. What kind of revision could be considered

4.1. Is there (still) any need for net neutrality rules?

In a context of crucial technological and market evolutions, a primary reflection should be devoted to whether net neutrality rules are still needed or whether there is room for an efficient radical reform of the principles underlying the current OIR.

In addition to more recent changes, many of the economic effects of Net Neutrality rules have never been fully considered, *ab origine*, by the current EU legislation. Indeed, the OIR looked at net neutrality as a policy almost exclusively concerning protection of end-users' rights, which of course is a paramount objective, yet not the sole one.

Indeed, due to this defect, some economic analysis really questioned at the basis the positive impact of net neutrality rules. In this regard, some economic literature has focused on the question of whether a competitive IAS market could make net neutrality rules (e.g., prohibition of payment against a "fast lane") redundant in terms of preventing anti-competitive behaviour. Recent theories have generally supported the

[66] In some member states, there have been proposals to extend entry and access/interconnection regulation to NIICS, e.g., in Italy, where now, the national transposition of EECC defines a third intermediary category of Interpersonal Communications Services, i.e., «ICS that makes an indirect use of numbering resources», which is an ICS that uses as identifier numbering resources assigned to another authorised operator.

[67] P. Larouche, *Network Neutrality: The Global Dimension,* in M. Burri-T. Cottier (eds.), *Trade Governance in the Digital Age: World Trade Forum,* Cambridge, 2012, 91 ss.

idea that lifting net neutrality rules on competing platforms is welfare-increasing.[68] Competition may influence the desirability of net neutrality provision concerning investments in broadband capacity and content innovation. In allowing a payment fast lane, both would increase compared to a net neutrality regime.[69] Empirical contributions are few, yet a very recent literature review shows that net neutrality regulations have negative impacts on high-speed network investment by (wireline) ISPs, which is in line with most theoretical contribution, and, in the long term, is likely to imply negative welfare effects. [70]

Nevertheless, a balanced assessment must not fall in the opposite extreme and overlook some of the core objectives of net neutrality rules, i.e., maintaining an open internet and protecting consumer freedom of choice for contents. For example, particular attention should be given to safeguarding audio-visual media services of general interest.[71] Indeed, «protecting and promoting a neutral and open Internet where content, services, and applications are not unjustifiably blocked or degraded» [72] should remain an overarching objective for the Digital Decade.[73] So, the main point is to aim for rules which allow to achieve these objectives, by minimising the distortive impact on economic and market dynamics.[74] In other words, net neutrality rules should embrace a general principle of the EU law: the "proportionality principle", which is also a well-recognised for the supply side access regulation in the sector.[75]

On the contrary, the OIR and its interpretation clearly moved away from that approach by adopting a "precautionary principle", thus imposing a strong restriction on regulated entities in view of a maximum probability of effectiveness. However, this approach inevitably leads to the risk of increased costs for the regulated company,

[68] This outcome is not due to competition reducing the incentives of ISPs to discriminate between content providers, as in the voice call termination, but to the intense competition among ISPs resulting in better prices for end-users and lower overall price distortions.

[69] M. Bourreau-F. Kourandi-T. Valletti, *Net Neutrality with Competing Internet Platforms*, in *Journal of Industrial Economics*, 63(1), 2015, 30 ss.

[70] W. Briglauer-K. Gugler-C. Cambini-V. Stocker, *Net neutrality and high-speed broadband networks: evidence from OECD countries*, in *European Journal of Law and Economics*, 55, 2022, 533 ss.; W. Briglauer, *Efficiency and Effectiveness of Net Neutrality Rules in the Mobile Sector,* cit.

[71] As for the prominence principle foreseen under art. 7a of the AVMSD and recital 29 of directive 2018/1808/EU. This is because of essential role that AVMS of general interest play in driving media pluralism, freedom of speech and cultural diversity. That special status is very often associated, at national level, with further obligations (such as the provision of newscasts) to better pursue those values and general interest objectives.

[72] EU Parliament, Council and Commission, *European Declaration on Digital Rights and Principles for the Digital Decade*, 2023.

[73] See for example G. De Minico, *Net neutrality e le generazioni future*, in M.R. Allegri-G. D'Ippolito (eds.), *Accesso a Internet e neutralità della rete fra principi costituzionali e regole europee,* Rome, 2017, 159 ss.

[74] For a similar approach, see P. Damiani, *The open Internet vs. net neutrality and the free Internet,* in *Federalismi.it,* 8, 2019.

[75] The proportionality principle is a general EU law principle, especially when it comes to economic regulation. Under art. 5(4) TEU, it applies at macro level for the definition of the scope of regulation (in the law-making process), yet this principle always applies at micro level as well, in the enforcement activity, for instance for the access regulation in the EECC, e.g., art. 68(2) «In accordance with the principle of proportionality, a national regulatory authority shall choose the least intrusive way of addressing the problems identified in the market analysis».

inefficiencies in the market and social costs.

A balanced and future-proof call for a neutral network should involve a proportional, dynamic, and systemic response to issues originating from digitalisation, multimedia convergence, network virtualisation and the overall modular structure of the current digital ecosystem.

Here, the idea of 'ne(x)t neutrality', that is to define rules aimed to cover all contexts of opacity and non-discrimination in each of the relationships constituting the digital transaction, by assessing substitutability and complementarity of services and preventing or counteracting exertions of power across the whole digital extended value chain, thus considering all the network and ecosystemic effects. Indeed, each digital transaction in the digital ecosystem is multifaceted and entails an array of interdependent bilateral relationships, namely: (i) end-user to end-user (one of which could be a business-user); (ii) end-user to ISP; (iii) End-user (and business user) to CAP; and (iv) ISP to CAP.[76] Non-discrimination and transparency principles should be applied to each of the above relationships, reflecting a different side of net neutrality. If regulation focus only on one specific side, by imposing strict rules, whereas do not focus on others (or develops rules in an uncoordinated way) it neglects existing interdependences and trade-offs or, worse, unintentionally generate or enhance contractual or market power situations elsewhere.[77]

Ne(x)t neutrality rules and their implementation should therefore be much closer to market analysis and pro-competitive regulation, including the key role played in the market by empowered consumers and end-users.[78]

From what described, it is evident that (i) end-user to ISP relationships have been profoundly disciplined for more than two decades by the EECC (as well as ISP to ISP competitive relationship), (ii) End-user to CAP have started to be regulated recently by the digital legislation (e.g., DSA, P2B, DMA, including also business users[79]) due to the need to discipline very large platforms CAPs market and bargaining power; whereas (iii) ISPs to CAPs are still only regulated, in an asymmetric fashion, by the OIR. This is because ISPs are not business users for digital platforms, so neither the P2B nor the DMA are disciplining that kind of transaction and interactions. [80]

On the contrary, telecom networks could be somehow considered intermediating between end-users and CAPs: some consider telecommunications networks to be a two-sided market, as telco operators sell both connectivity services to end-users and

[76] Being the first one (i) end-user to end-users related to interaction of social network, iv), in turns, itself multifaceted and complex, involving (i) substitutability; (ii) cooperation and (ii) complementarity relationships BoR (24) 51

[77] For a similiar "preliminary" concern, see M. Orofino, *La declinazione della net-neutrality nel Regolamento europeo 2015/2120. Un primo passo per garantire un'Internet aperta?*, cit.

[78] A. Manganelli-A. Nicita, *The governance of telecom Markets*, cit.

[79] Platforms' business users have a twofold regulatory framing: on one side, they are considered as users, as they actually uses platforms services to reach end-users; yet, they are also considered as potential competitors in the digital ecosystem, where platforms vertically integrate.

[80] As a matter fact, possibly, art. 6(6) of the Digital Markets Act (DMA) would limit CAPs' discrimination vis à vis ISPs, but only if those "contents and applications" can be qualified as one of the core platform services and those companies are qualified as gatekeepers.

termination services for content and application providers.[81]

4.2. Amending net neutrality regulation: few proposals

A rethinking of OIR rules could be considered, as mentioned, according to principles of ne(x)t neutrality: proportionality, systemic perspective, and end-user's empowerment.

In this respect, policymakers should anyway consider that competition among ISPs tends to provide a safeguard against severe rent extraction and, thus, an abuse of throttling as an exploitative device. Therefore, enforcement of net neutrality rules should always account for the competitive environment, under a proportionality approach. As a general concept, updating net neutrality rules would allow possibilities to differentiate quality which could be beneficial for ISPs, as giving room to move away from pure price competition and allow consumers wider choices for better matching their preferences.

One interesting reference about updating net neutrality obligations is given by the recent Ofcom statement.[82] In this line, Ofcom underlines that ISPs should be able to offer premium quality services, at a premium price, differentiated from standard quality ones, at a more affordable price, in order to better meet differentiated costumers' needs (i.e., customers using high-quality virtual reality application vs users that only browse the internet). This is in line with the current BEREC concept of 'application-agnostic offer', as this differentiation applies to all the content and services accessed by consumers purchasing the offer. ISPs should be also probably allowed to indicate that all content and application with certain characteristic (e.g., on demand video streaming at very-high definition, 4k) could be available only with some premium package, therefore linking it to the concept of «objectively different technical QoS requirement of traffic categories». If those categories of traffic are related with "premium" content/service, charging an additional price to users, a commercial equilibrium between the IAS and Content/Application prices for users could be found – even by possibly framing and considering the differential premium service as a particular form of Premium Rate Service (PRS).[83]

Moreover, in its statement, Ofcom allows zero-rating offers that are genuinely open to all content providers offering similar services and contents ("class-based offers"), e.g., video streaming content, audio streaming content or social media. Further to that, ISPs should be probably allowed to build retail offers where specific content is treated differently ('content-specific retail offers') when consumers choose for such a differentiation, selecting the specific content (that could be made available by CAPs in a "premium" fashion).

An end-user-empowering approach to net neutrality could be the best way to guarantee a freedom of choice, by allowing the end-users to decide what kind of internet

[81] B. Julien-M. Bouvard, *Fair cost sharing: big tech vs telcos,* 2023, TSE wp n 1376.

[82] Ofcom, *Net Neutrality review*, cit.

[83] *About PRS see ofcom.org.uk*.

access they would prefer, without over restricting the economic and commercial freedom of companies. As the current rules stands, ISPs are restricted to offering only basic packages of service, that ultimately lead, in some circumstances, to limit rather than enhancing consumer choice, and to have some customers subsidising others (e.g., normal vs heavy users). Whereas an enhanced flexibility for operators would give them incentives to innovate and create more bespoke and dynamic services, thus benefiting consumers' choice and welfare and also helping to address their investment needs.

As long as customers truly have a choice – i.e., a competitive market environment and the existence of a portfolio of tariff options and comparable plan where all content is unthrottled or not blocked – consumers could be allowed to voluntarily opt for differentiating certain traffic categories.[84] A simple solution could be to introduce an application-agnostic 'anchor product' which all users can choose if they want. With that in place, ISPs can offer all type of differentiated services in addition to that, without affecting, yet enhancing, consumers' freedom of choice. If users expressly choose those alternatives, it means they are better off than with the anchor product. This approach should prevail over the concept of compulsory application-agnostic offer, which at the end could be limit consumer sovereignty and empowerment, not allowing them to reach those contents with that differentiated quality they would prefer. In this regard, it should be reminded that OIR art. 3(1) protection apply to all end-users, comprising both consumers and businesses.[85]

In other words, there is a trade-off between art. 3(1) and art. 3(3) of OIR, requiring some balancing and a end-user-empowering approach to net neutrality seems a balanced solution allowing to reach the most efficient outcome.

In this regard, it seems important to underline that the same art. 3(1) of the OIR gives end-users the possibility to choose for their own terminal equipment,[86] which is considered a fundamental element of net neutrality. Therefore, it would be quite incoherent to consider end-user enough sophisticated and well informed to take advantage from a personal choice of terminal equipment (if they prefer not to buy and use the default standard product supplied by ISP), which is a quite technical and sophisticated choice, where, at the same time, considering in a negative way a possibility for them to choose how their connection could be configured in terms of type of traffic and prioritisation (should they want to have another configuration).

This consumer-empowering approach to net neutrality should be possible also for zero-rating practices when the end-users select the applications or contents for which

[84] J. Kramer-M. Peitz, *A fresh look at zero-rating*, in *Telecommunications Policy*, 42(7), 2018, 501 ss.

[85] Art. 2(14) EECC defines end-users, as those natural or legal persons using or requesting publicly available electronic communications services, thus comprising also businesses, yet only those not providing in turn public electronic communications networks or publicly available electronic communications services.

[86] Equipment that directly or indirectly connect to the interface of a public network. This interface, the Network Termination Point (NTP), is defined as the physical point at which a subscriber is provided with access to a public communications network. The location of the NTP has an impact on whether the router and modem are part of the IAPs' network or end-users can use their own equipment to access the Internet. In this regard, abovementioned BEREC guidelines have dealt with this issue, and more specifically also BEREC, *Report on the Location of the Network Termination Point* and BEREC, *Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies*.

data usage is not subtracted from his data allowance. This selection should be transparent and non-discriminatory meaning that all contents and applications could be potentially chosen by end-users for the "premium" treatment. If access to zero-rated partner programmes is non-discriminatory and entails low barriers to entry, a sound theory of harm for content providers will usually not be given.[87]

Finally, it is important to stress again that, in this consumer-empowering vision for NN, likewise for the general consumer empowerment, the transparency provisions are of paramount importance, yet a unified approach with consumer empowerment rules in the EECC should be necessarily carried out.

5. Conclusion

Net neutrality rules are a very peculiar type of regulation promoting end-users' interest in the electronic communications industry and this paper aimed at building a case for a rethinking of the existing rules in Europe. This consideration is based onto a few reasons.

First, as a general point, demand-side pro-consumer policies should be designed and implemented also considering efficiency objectives and their competitive impact. On this basis, it seems appropriate to have a re-thinking of the net neutrality rules, as the original approach embraced by the EU open internet regulation was based solely on a legalistic consumer protection rationale, which could prove to be inefficient, creating disadvantages for consumers, too.

This is even more relevant in a context of increasing interdependences between the electronic communication service and network providers and the other actors active in what could be considered an extended digital network and services value chain. Here it is a second motivation for re-thinking the current rules: while an increasing digital legislation has reconsider the role and interplay of the different actors in the digital ecosystem, i.e., between very large CAPs and end-users, on one side, and business-users, on the other side, it would be completely ideological not to re-assess the rules concerning the main relationships between Internet service providers (ISPs) and content and application providers (CAPs).

Finally, another broad yet crucial aspect should be considered: within the current EU digital industrial policy, ambitious connectivity targets (supply of electronic communications high-speed networks) have been developed by the EU policy maker.[88] Those

[87] J. Kramer-M. Peitz*, A fresh look at zero-rating,* cit.

[88] With emergence of new technologies, the EU public policy for the electronic communications markets began to gradually focus on industrial policy issues, such as the extensive development of future-proof technological assets. The EU progressively designed industrial policies for new investments, by setting connectivity and ultra-broadband targets. At the European level, these industrial policies have been raised from the goals established within the 2010 Digital Agenda for Europe (DAE) to the ambitious objectives within the 2016 Gigabit Society (GS). In the 2016 GS, the Commission set out the following connectivity objectives for 2025: (a) all Union households, rural or urban, should have an internet connectivity with a download speed of at least 100 Mbps, upgradable to 1 Gbps; (b) socio-economic drivers, such as digitally intensive enterprises, schools, hospitals and public administration should benefit from a download speed of at least 1 Gbps and an upload speed of at least 1 Gbps; and

targets and the consequent public funding devoted to augmenting private companies' investment capacity assume that «there is a link between the increased deployment of fixed and mobile broadband and economic development … higher speeds and new generations of mobile networks have a positive impact on GDP».[89] Therefore, the current EU industrial policy assumes that there are positive externalities across the digital ecosystem correlated with the deployment and provision of very high-capacity (VHC) telecom networks.[90]

In economic terms, positive externalities imply indirect benefits to individuals/companies for which the externalities' producers are not compensated because those benefits are external to the market(s) where that producers operate. In other words, private benefits (for the actors in the market considered) are lower than social benefits (outside that market) and therefore there is an under-provision of that service/goods. To realign social and private benefits, in order to enhance social welfare, the activity producing positive externalities should be incentivised and increased, by internalising those positive externalities.

In this context, the notorious discussion on "fair contribution" stands, dealing with how to transfer some monetisation from content to networks in order to efficiently internalise positive externalities that telcos are producing in an extended ecosystem and are exploited by large digital platforms. «So that all market actors benefiting from the digital transformation assume their social responsibilities and make a fair and proportionate contribution to the costs of public goods, services and infrastructures, for the benefit of all people living in the EU».[91]

Without entering in this very complex and controversial issue, it can be highlighted that, on one side, complementarity between internet access services and content weakens a pure "free riding" argument linked to a positive externalities' environment, as positive externalities are somehow reciprocal due to the positive impact on demand of internet access services that digital contents (especially must-have contents) exert. On the other side, however, IAS subscriptions and digital contents may not be perfect complements at all.[92]

(c) all urban areas and major transport paths should have uninterrupted 5G coverage

[89] EU Commission, White paper, cit.

[90] Quite a few empirical analyses recognise a positive causal effect of the deployment of telecommunications networks and services on GDP growth. See, for example, L.H. Roller-L. Waverman, *Telecommunications Infrastructure and Economic Development: A Simultaneous Approach*, in *American Economic Review*, 91(4), 2001, 909 ss.; and N. Czernich- O. Falck- T. Kretschmer-L. Woessmann, *Broadband Infrastructure and Economic Growth*, in *The Economic Journal,* 121, 2011, No. 552, 505 ss. In addition, recent studies, specific to fibre investments in Italy, have shown that the use of ultra-fast connections has positive effects on both the productivity of firms and on market dynamics, favouring the entry of new firms in sectors with greater use of digital technologies. See C. Cambini-E. Grinza-L. Sabatino, *Ultra-fast broadband access and productivity: Evidence from Italian firms,* in *International Journal of Industrial Organization*, 86, 2023 and C. Cambini-L. Sabatino, *Digital highways and firm turnover,* in *Journal of Economics and Management Strategy,* 2023, 1 ss.

[91] European Declaration on Digital Rights and Principles for the Digital Decade

[92] This is mainly because, even if demand of connectivity is substantially driven by content consumption, the decision for end-users to subscribe to an ISP (i) may come also from a few different reasons (e.g., interpersonal communications); and (ii) is a preliminary (autonomous) choice in a two-step approach (whereas for typical complementary products users decide, at the same time, how much to buy in

In any case, in economic theory, positive externalities could be tackled '*à la Pigou*', i.e., by providing contributions aimed at internalising those externalities and re-align social and private benefits. However, those externalities can also be tackled '*à la Coase*', i.e., by reducing transaction costs and letting the parties to freely negotiate within the ecosystem.

As described, net neutrality rules, given the current market conditions, create insurmountable transaction costs within the ecosystem by qualifying many possible transactions between telcos and CAPs as illicit, thus making it very difficult to use Coesian market-based solutions. Indeed, exactly an inflexibility in the net neutrality approach is at the very base of the endless controversy on "fair-contribution". On the contrary, as proposed, a substantial softening of the transactional constraints imposed by net neutrality rules may allow using market mechanisms to address externalities and therefore possibly tackling under-provision of (network) services.

function of both products prices); and therefore (iii) the consumption of contents can be variable within a constant demand for connectivity. Therefore, in case of a price increase for contents there will be less consumption of contents and not necessarily also a decline in the IAS demand. Symmetrically, when a decrease in contents price takes place, this will not be necessarily followed by an increase in connectivity demand yet rather an increase in content demand.

La funzione di *public cybersecurity* come preminente funzione pubblica digitale alla luce della Direttiva NIS2*

Alfonso Contaldo

Abstract

Il cyberspazio è una sorta di non luogo di progettazione matematica in cui oramai si svolgono molte attività umane aventi anche rilevanza economica e finanziaria ed in cui lo Stato si attiva per garantirvi soprattutto la funzione di Pubblica sicurezza, che in riferimento alle attività di governo statale e di livello centrale e locale necessitano di un complesso di apparati, autorità e strutture preposte alla tutela dell'ordine pubblico e all'incolumità delle persone.
La pubblica sicurezza nel cyberspazio riguarda tanto le attività di polizia, volte ad assicurare la "sicurezza" attraverso il rispetto delle norme di legge, quanto quelle comunque finalizzate a "prevenire" che la comunità possa patire danni da eventi fortuiti e accidentali, infortuni e disastri di qualunque altro genere.

Cyberspace is a sort of non-place of mathematical planning in which many human activities now take place which also have economic and financial relevance and in which the State takes action to guarantee above all the public security function, which in reference to the activities of state government and at a central and local level require a complex of apparatus, authorities and structures responsible for the protection of public order and the safety of people.
Public safety in cyberspace concerns both police activities, aimed at ensuring "safety" through compliance with the law, and those aimed at "preventing" the community from suffering damage from fortuitous and accidental events, accidents and disasters. of any other kind.

Sommario

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

d. lgs. n. 138 del 2024. - 4. L'Agenzia per la Cybersecurity Nazionale e l'esercizio delle funzioni di vigilanza sul cyberspazio. - 5. Brevi conclusioni: il cyberspazio come non luogo di intervento dello Stato per la "pubblica sicurezza digitale".

Keywords

cyberspazio – Stato – pubblica sicurezza – prevenzione – danni digitali

1. Il ciberspazio come "ambito spaziale" per le funzioni pubbliche digitali

Il Ciberspazio è il "luogo" nel quale sembra accadere una trasmissione telematica anche *point to point*.[1] Lo "spazio" nel ciberspazio possiede gli aspetti in comune con l'astratto significato matematico del termine piuttosto che con lo spazio fisico: il significato spaziale può essere attribuito alla relazione tra i *bit*. Il concetto di ciberspazio quindi si riferisce non al contenuto presentato al navigatore, ma piuttosto alla possibilità di navigare tra differenti siti, tramite i cicli di *feedback* tra l'utente ed il resto del sistema (in una soluzione matematica), che crea così la possibilità potenziale di incontrare sempre qualcosa di inatteso e sconosciuto e pertanto lo stesso ciberspazio diventa una sorta di "non luogo" (come soluzione matematica), prescindendo dal contatto personale tra soggetti e consentendo agli utenti, attraverso l'uso di strumenti assai diffusi non solo tra gli *hacker* e i *cracker* di agire nel pieno anonimato, anche durante la pandemia del Covid ad organi costituzionali[2].

Ciò spiega perché l'ordinamento statuale, da alcuni anni a questa parte, stia tentando di garantire in tale ambito il rispetto delle norme giuridiche nazionali[3], l'esercizio di pubbliche funzioni e la repressione di eventuali crimini[4], oltreché l'ingerenza sulla corretta fruibilità dello stesso. Ciò spiega perché nel ciberspazio lo Stato vi operi per il rispetto del suo ordinamento giuridico con settori specializzati delle forze di polizia, con la difesa da attacchi di *cyberwarfare* da raggruppamenti specializzati delle Forze Armate (non da "armi" vere e proprie), mentre le *policies* della "difesa" del ciberspazio viene garantita dall'Agenzia per la Cibersecurity Nazionale (ACN)[5]. Il ciberspazio afferente allo Stato italiano non è quindi un "territorio" difeso da una Forza armata,

[1] Vedi B. Sterling, *Giro di vite contro gli hacker*, Boston, 2015, 122 ss.

[2] Vedi P. Marsocci, *Lo spazio digitale dei lavori parlamentari e l'emergenza sanitaria Covid-19*, in questa *Rivista*, 2020, 2, 52 ss.

[3] Vedi A. Venanzoni, *Sovranità tra ordine costituzionale, digitale e poteri privati*, in M. Proietti-A. Venanzoni, *La sovranità digitale fra sicurezza nazionale e ordine costituzionale*, Pisa, 2023, 137 ss.

[4] Vedi A.C. Amato Mangiameli, *Reato e reati informatici. Tra teoria generale del diritto e informatica giuridica,* in A.C. Amato Mangiameli-G. Saraceni, *I reati informatici. Elementi di teoria generale e principali figure criminose*, Torino, 2019, 27 ss.

[5] Vedi M.F. Dos Santos-A. Contaldo, *L'Agenzia per la cybersicurezza nazionale: istituzione e problematiche in campo*, in *Riv. amm. Rep. it.,* 5/6, 2022, 343 ss.; G.G. Cusenza, *I poteri dell'Agenzia per la Cybersicurezza Nazionale: una nuova regolazione del mercato cibernetico*, in R. Ursi (a cura di), *La sicurezza nel cyberspazio,* Milano, 2023, 123 ss.

come lo sono la terra (Esercito), l'aria (Aeronautica militare), il mare (Marina militare), ma una sorta di "non luogo" di struttura matematica avente rilevanza economica anche per la criminalità[6] dove il rispetto dell'ordinamento è garantito dalle attività delle forze di polizia (Polizia di Stato, Carabinieri, Guardia di Finanza), dalle agenzie per la sicurezza nazionale (AISI, AISE) e la cui fruibilità corretta è garantita rispetto a pratiche che danneggerebbero gli *asset* da un'apposita agenzia (Agenzia per la Cibersecurity Nazionale), mentre le Forze armate rispondono agli attacchi di *cyberwarfare*. Sembra così definirsi una sorta di Stato digitale che riporta in codice binario diverse sue attività e competenze pur non riducendosi ad esse[7].

2. La vigilanza, l'esecuzione e la giurisdizione sul "cyberspazio nazionale"

La Direttiva NIS 2 (direttiva (UE) 2022/2555) disciplina altresì la giurisdizione e la "competenza" (anche se sulla previsione di un ambito cibernetico, sul quale non è mai intervenuto finora il diritto internazionale), dall'art. 26 e seguenti indicando che i soggetti che rientrano nel suo ambito di applicazione debbano essere «considerati sotto la giurisdizione dello Stato membro nel quale sono stabiliti».

A questo principio, la prima e più evidente eccezione riguarda i fornitori di reti pubbliche di comunicazione elettronica o i fornitori di servizi di comunicazione elettronica accessibili al pubblico, poiché in entrambi i casi considerati sono posti sotto la giurisdizione dello Stato membro nel quale forniscono i loro servizi a prescindere dal luogo dove essi sono stabiliti[8].

La seconda eccezione, invece, più prosaicamente prevede che per la libera circolazione dei servizi debbano essere considerati sotto la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione europea alcune categorie di soggetti tassativamente elencate: a) i fornitori di servizi DNS; b) i registri dei nomi di dominio di primo livello; c) i soggetti che forniscono servizi di registrazione dei nomi di dominio; d) i fornitori di servizi di *cloud computing*; e) i fornitori di servizi di data center; f) i fornitori di reti di distribuzione dei contenuti; g) i fornitori di servizi gestiti; h) i fornitori di servizi di sicurezza gestiti; i) i fornitori di mercati online; l) di motori di ricerca online o di piattaforme di servizi di social network.

In relazione a tale seconda eccezione, al fine di determinare se un soggetto ha il proprio stabilimento principale nell'Unione europea, non sono criteri decisivi la presenza e l'utilizzo dei sistemi informativi e di rete, poiché occorre avere riguardo allo Stato membro in cui sono prevalentemente adottate le decisioni relative alle misure di gestione del rischio di cibersicurezza. Nel caso in cui non sia possibile individuare lo Stato membro si dovrà applicare il successivo criterio secondo il quale lo stabilimento principale è quello nello Stato membro in cui sono effettuate le operazioni di cibersi-

[6] Vedi S. Pietropaoli, *Informatica criminale*, Torino, 2023, 81 ss.

[7] Vedi L. Torchia*, Lo Stato digitale. Un'introduzione*, Bologna, 2023, 72 ss.

[8] Ci si permette di rinviare al nostro *L'attuazione della* cybersecurity *nazionale: un difficile esercizio di una funzione pubblica*, in *Lo Stato*, 2023, 21, 283 ss.

curezza[9]. Per *extrema ratio*, si applica un terzo criterio, ossia che lo stabilimento principale venga determinato dalla sede con il maggior numero di dipendenti nell'Unione europea[10] .

Con riferimento alla suddetta seconda eccezione è, altresì, prevista la designazione di un rappresentante nell'Unione europea per il soggetto che senza esservi stabilito offra servizi nel territorio di uno Stato membro. E' stato ricordato[11] come ai sensi dell'art. 6, n. 34, della Direttiva NIS 2 il "rappresentante" sia una persona fisica o giuridica stabilita nell'Unione europea, espressamente designata ad agire per conto di un fornitore di servizi DNS, un registro dei nomi TLD, un soggetto che fornisce servizi di registrazione di nomi di dominio, un fornitore di servizi di *cloud computing*, un fornitore di servizi di *data center*, un fornitore di reti di distribuzione dei contenuti, un fornitore di servizi gestiti, un fornitore di servizi di sicurezza gestiti, o un fornitore di mercato online, di un motore di ricerca online o di una piattaforma di servizi di *social network* che non è stabilito nell'Unione europea, a cui l'autorità nazionale competente o un CSIRT può rivolgersi in sostituzione del soggetto in questione per quanto riguarda gli obblighi posti in capo a quest'ultimo dalla stessa Direttiva NIS 2 .

Quindi il rappresentante è considerato come "stabilito" in uno degli Stati membri in cui sono offerti i servizi, con la conseguenza che il soggetto rappresentato a sua volta sarà sotto la giurisdizione dello Stato membro in cui il suo rappresentante si è stabilito. La mancata designazione del rappresentante nell'Unione europea non è priva di conseguenze. Essa, infatti, ai sensi dell'art. 26, costituisce una violazione degli obblighi previsti dalla Direttiva NIS 2 e «qualsiasi Stato membro in cui il soggetto fornisce servizi» ha il potere di promuovere nei suoi confronti un'azione legale davanti alla Corte di Giustizia; la designazione del rappresentante fa salve le azioni legali che potrebbero essere avviate nei confronti del rappresentato.

Gli Stati membri che hanno ricevuto una richiesta di assistenza reciproca in relazione a uno dei soggetti con stabilimento principale nell'Unione europea possono, entro i limiti di tale richiesta, adottare misure di vigilanza e di esecuzione adeguate in relazione al soggetto interessato che nel loro territorio fornisce servizi oppure ha un sistema informativo e di rete. La terza e ultima eccezione al principio di stabilimento, sancito dal sopramenzionato art. 26, primo paragrafo, della Direttiva NIS 2, è rappresentata dagli enti della pubblica amministrazione. Secondo la direttiva in parola per «ente della pubblica amministrazione» si intende: un soggetto riconosciuto come tale in uno Stato membro conformemente al diritto nazionale che soddisfa i seguenti criteri: a) è istituito allo scopo di realizzare esigenze di interesse generale ed è privo di carattere industriale o commerciale; b) è dotato di personalità giuridica o autorizzato per legge ad agire a nome di un altro soggetto che ne è dotato; c) è finanziato in prevalenza dallo Stato, da autorità regionali o da altri organismi di diritto pubblico, la sua gestione

[9] Le operazioni di cybersicurezza diventano così una sorta di stabilimento. Sul punto *Ibid.* e, soprattutto, S. Marchiafava, *Giurisdizione, vigilanza ed esecuzione*, in C. Cavaceppi-A. Contaldo (a cura di), *Cybersecurity connect*, Roma, 2024, 254 ss.

[10] Ma ciò richiede che la previsione di un perimetro cibernetico delle imprese sia attivata da tutti gli Stati europei. Vedi L. Calandriello, *Il perimetro di sicurezza nazionale cibernetica*, in R. Ursi (a cura di), *La sicurezza*, cit., 136 ss.

[11] Ancora S. Marchiafava, *Giurisdizione*, cit., 254 ss.

è soggetta alla vigilanza di tali autorità o organismi, oppure è dotato di un organo di amministrazione, di direzione o vigilanza, in cui più della metà dei membri è designata dallo Stato, da autorità regionali o da altri organismi di diritto pubblico; d) ha il potere di adottare, nei confronti di persone fisiche o giuridiche, decisioni amministrative o normative che incidono sui loro diritti relativi alla circolazione transfrontaliera delle merci, delle persone, dei servizi o dei capitali. Sono esclusi dalla definizione di ente della pubblica amministrazione: la magistratura, i parlamenti e le banche centrali. Tali enti sono, infatti, considerati posti sotto la giurisdizione dello Stato membro che li ha istituiti.

Assumono, inoltre, un ruolo centrale gli obblighi in materia di vigilanza ed esecuzione previsti in capo agli Stati membri dalla Direttiva NIS 2.

Di qui anche l'esigenza di imporre agli Stati membri: (a) la designazione di una o più autorità nazionali competenti in materia di cibersicurezza per lo svolgimento dei compiti di vigilanza previsti dalla Direttiva NIS 2; (b) l'individuazione del Single Point Of Contact (SPOC) con funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità degli Stati membri[12].

Ai sensi dell'art. 8 della Direttiva NIS 2, ogni Stato membro designa o istituisce una o più autorità competenti responsabili della cibersicurezza e dei compiti di vigilanza disciplinati dal settimo capo VII, nonché sul controllo per quanto riguarda l'attuazione della stessa direttiva a livello nazionale[13], istituendo un Punto Unico di Contatto che svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità del relativo Stato membro con le omologhe autorità degli altri Stati membri, e, ove opportuno, con la Commissione e l'ENISA[14], nonché per garantire la cooperazione intersettoriale con altre autorità competenti dello stesso Stato membro. Diviene, altresì, compito degli Stati membri assicurare alle rispettive autorità nazionali competenti e ai propri punti di contatto unici, le risorse adeguate a svolgere i compiti loro assegnati e conseguire, quindi, gli obiettivi della Direttiva NIS 2.

Tra le novità anche l'introduzione di un regime di vigilanza ex post applicato a un numero di nuovi soggetti denominati «soggetti importanti». La Direttiva NIS 2 ha l'obiettivo di rendere il livello di *cybersecurity* di operatori considerati «essenziali» e «importanti» uniforme su tutto il territorio europeo. Nella prima categoria troviamo anche le pubbliche amministrazioni, in aggiunta agli operatori del settore energetico, sanitario, spaziale, bancario, dei trasporti, delle infrastrutture digitali, delle acque. Nella seconda categoria troviamo i soggetti importanti, cioè gli operatori di servizi postali e corriere, di gestione dei rifiuti, del settore chimico, del settore agroalimentare. Tale distinzione tra soggetti essenziali e soggetti importanti, contemplata dall'art. 3 della Direttiva NIS 2, rappresenta una delle novità più significative.

La Direttiva NIS 2 contraddistingue tra un regime di vigilanza ex ante per i soggetti essenziali e un regime di vigilanza *ex post* per i soggetti importanti; tale ultimo regime

[12] Ci si permette di rinviare al nostro *L'attuazione*, cit., 294 ss.

[13] Ancora S. Marchiafava, *Giurisdizione*, cit.

[14] Ci si permette di rinviare al nostro *L'ENISA e le competenze comunitarie per la cibersicurezza, in Riv. polizia*, 6/7, 2018, 655 ss.

impone alle autorità competenti di adottare provvedimenti quando ricevono elementi di prova o indicazioni che un soggetto importante non soddisfa i requisiti di sicurezza e di segnalazione degli incidenti.

Gli Stati membri devono imporre alle rispettive autorità competenti di monitorare e di vigliare lo stabilimento, imponendo ovviamente di adottare le misure necessarie per garantire l'osservanza[15] della Direttiva NIS 2: pertanto in un approccio basato sul rischio, le autorità nazionali competenti stabiliscono metodologie che permettono di conferire priorità ai compiti di vigilanza esercitati ai sensi degli artt. 32 e 33 della stessa Direttiva NIS 2. Quindi nei casi di incidenti che determinano la violazione di dati personali è contemplata una specifica e stretta collaborazione tra le autorità competenti secondo la Direttiva NIS 2.

Riguardo agli enti della pubblica amministrazione, tenuti all'osservanza della Direttiva NIS 2, gli Stati membri devono attribuire alle rispettive autorità, in Italia la ACN[16], poteri adeguati e un'indipendenza operativa in relazione alle misure di vigilanza e di esecuzione da imporre a tali enti conformemente ai quadri legislativi e istituzionali nazionali.

Con l'art. 5 del d. lgs. 4 settembre 2024 n. 138 si ribadisce che vengono sottoposti alla giurisdizione nazionale i soggetti di cui all'art. 3 dello steso decreto legislativo stabiliti sul territorio nazionale, ad eccezione degli stessi medesimi casi già previsti dalla direttiva (UE) 2022/2555 (i fornitori di reti pubbliche di comunicazione elettronica o i fornitori di servizi di comunicazione elettronica accessibili al pubblico; i fornitori di servizi di sistema dei nomi di dominio DNS, i registri dei nomi di dominio di primo livello, i soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di *cloud computing*, i fornitori di servizi di *data center*, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online o di piattaforme di servizi di social network, che sono sottoposti la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione; gli enti della pubblica amministrazione). Si considera altresì lo stabilimento principale nell'Unione quello dello Stato membro nel quale sono prevalentemente adottate le decisioni relative alle misure di gestione del rischio per la sicurezza informatica. Se non è possibile determinare lo Stato membro in cui sono adottate le suddette decisioni o se le stesse non sono adottate nell'Unione, lo stabilimento principale è quello collocato nello Stato membro in cui sono effettuate le operazioni di sicurezza informatica. Nel caso di soggetti non stabiliti nel territorio dell'Unione ma offrono servizi all'interno dello stesso, essi debbono designare un rappresentante nell'Unione, che è stabilito in uno degli Stati membri in cui sono offerti i predetti servizi ed è sottoposto alla relativa giurisdizione. In caso di mancanza della designazione del rappresentante, l'ACN può avviare un'azione legale, nei confronti dei soggetti inadempienti, anche se non appartenenti al Perimetro Nazionale di Sicurezza Cibernetica, che viene quindi a ricevere una possibile integrazione.

---

[15] Vedi I. Forgione, *Il ruolo strategico dell'Agenzia Nazionale per la Cybersecurity nel contesto del Sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in R. Ursi (a cura di), *La sicurezza*, cit., 95 ss.

[16] Vedi G.G. Cusenza, *I poteri*, cit., 115 ss.

3. La delineazione Perimetro Nazionale di Sicurezza Cibernetica nella legge n. 133 del 2019 e il coordinamento con il d. lgs. n. 138 del 2024

Il Perimetro Nazionale di Sicurezza Cibernetica viene a definirsi come il "non luogo tecnologico" che insistendo sulla rete potrebbe anche concorrere al formarsi di una normativa internazionale che possa delineare il suo rapporto con gli ordinamenti statuali[17], venendo ad acquisire una più significativa connessione operativa con i soggetti che ne contribuiscono il suo sviluppo[18]. Quindi nell'attuale quadro normativo delle infrastrutture tecnologiche strategiche, in linea con le più elevate ed aggiornate misure di sicurezza adottate a livello internazionale, l'art. 1 del d.l. 21 settembre 2019, n. 105, così come modificato dalla legge 18 novembre 2019 n. 133, istituisce il cd. Perimetro Nazionale di Sicurezza Cibernetico come una modalità organizzativa al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per «il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale». Inoltre si ricorre alla previsione del regolamentazione attraverso i decreti del Presidente del Consiglio dei Ministri su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), per prevedere ai sensi dell'art. 1-bis del d.l. 15 marzo 2012, n. 21, il contemperamento delle disposizioni in materia di valutazione della presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti inerenti ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G[19] e dei dati che vi transitano con le misure volte ad individuare le attività di rilevanza strategica per il sistema di difesa e di sicurezza nazionale, fermo restando che, per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate, si applica quanto previsto dal regolamento adottato ai sensi dell'art. 4, c. 3, lett. l), della l. 3 agosto 2007, n. 124.
Il Presidente del Consiglio dei Ministri coordina la coerente attuazione delle disposizioni che disciplinano il Perimetro, anche avvalendosi del Dipartimento delle Informazioni per la Sicurezza, che assicura gli opportuni raccordi con le autorità titolari delle competenze sul settore e con gli altri soggetti interessati.
L'individuazione avviene sulla base di un criterio di gradualità, tenendo conto dell'en-

[17] Vedi G. Sartor, *La rivoluzione informatica e la globalizzazione*, in G. Torresetti (a cura di), *Diritto, politica e realtà sociale nell'epoca della globalizzazione* – Atti del XXII Congresso della Società Italiana di filosofia giuridica e politica, Macerata, 2008, 245 ss.

[18] Sulla disciplina normativa del perimetro nazionale cibernetico vedi S. Mele, *Il perimetro di sicurezza nazionale cibernetica e il nuovo "golden power". Dalla compliance delle aziende e della Pubblica amministrazione alla sicurezza nazionale*, in G. Cassano-S. Previti (a cura di), *Il diritto di internet dell'era digitale*, Milano, 2020, 185 ss.

[19] Ci si permette di rinviare al nostro, *La disciplina della sicurezza del perimetro cibernetico nazionale anche alla luce dello standard 5G*, in A. Contaldo-D. Mula (a cura di), *Cibersecurity law*, Pisa, 2021, 185 ss.; M. Matassa, *La regolazione della cybersecurity in Italia*, in R. Ursi (a cura di), *La sicurezza*, cit., 21 ss.

tità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziale, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici.

Anche se il ritardo temporale rispetto ai quattro mesi dalla l. 18 novembre 2019 n. 133 che ha convertito il decreto-legge istitutivo dell'Agenzia Nazionale della Cybersecurity[20], è stata data l'attuazione della potestà regolamentare in capo al Presidente del Consiglio di Ministri che su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR) ha adottato il dPCM 31 luglio 2020 n. 131, al di fine: a) di individuare le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal presente articolo; alla predetta individuazione, fermo restando che per gli Organismi di informazione per la sicurezza si applicano le norme previste dalla loro legge istitutiva (l. 3 agosto 2007, n. 124)[21], si procede sulla base dei peculiari criteri[22]; b) di definire i criteri in base ai quali i soggetti già predeterminati in precedenza predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, e nel provvedere all'elaborazione di tali criteri, adottando opportuni moduli organizzativi, sulla scorta di quanto previsto dall'organismo tecnico di supporto al CISR, integrato con un rappresentante della Presidenza del Consiglio dei ministri; c) di curare (sempre a carico dei suddetti soggetti) la trasmissione entro sei mesi dalla data di entrata in vigore del decreto in questione, la trasmissione di tali elenchi, rispettivamente, alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico (ora MIMIT), i quali a loro volta inoltrano gli elenchi di rispettiva pertinenza al Dipartimento delle Informazioni per la Sicurezza, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica, nonché all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, che ai sensi dell'art. 7 *bis* della l. 31 luglio 2005, n. 155, provvede sia ad assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate da un apposito decreto del Ministro dell'interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate, sia ad operare per la prevenzione e repressione delle attività terroristiche o di agevolazione del terrorismo condotte con i mezzi informatici, con gli ufficiali di polizia giudiziaria all'uopo incaricati anche in collaborazione con gli altri

[20] Vedi I. Forgione, *Il ruolo*, cit., 95 ss.

[21] Sul punto vedi F. Pastore, *Il coordinamento delle forze di polizia e di sicurezza italiane nella lotta al terrorismo*, in *Diritti fondamentali*, 2021, 2; P. Vipiana, *Introduzione al diritto della sicurezza pubblica*, Torino, 2022, 91 ss.; R. Ursi, *La sicurezza pubblica*, Bologna, 2022, 112 ss.

[22] Questi criteri vengono individuati nelle fattispecie nelle quali: 1) il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato; 2) l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale.

organi di polizia.
Il cyberspazio può, pertanto, essere considerato come delimitazione dello "Stato digitale", secondo una concezione elaborata dalla dottrina giusamministrativa per il quale l'apparato pubblico «continua, naturalmente, a svolgere tutte le funzioni e i compiti da esso precedentemente assunti, ma presenta due caratteristiche nuove rispetto al passato. Sotto un primo profilo, l'attività pubblica nel suo complesso viene trasformata, quanto a modi e strumenti, mediante l'applicazione di nuove tecnologie.
Che si tratti della sicurezza o dei servizi pubblici, della realizzazione di infrastrutture o dell'esercizio della giustizia, della moneta e della difesa, della salute o della pianificazione del territorio, si impone via via il ricorso a strumenti tecnologici che portano con sé sia una riarticolazione e riorganizzazione delle funzioni e delle strutture pubbliche, sia la ridefinizione delle regole di esercizio del potere pubblico e delle relative modalità di controllo. Sotto un secondo profilo, lo sviluppo tecnologico investe i rapporti economici e sociali in misura tale da rendere spesso inidonee o obsolete le regole vigenti. Di qui la necessità di una nuova regolazione pubblica volta ad aggiornare discipline già esistenti e a introdurre principi e regole nuove per fenomeni nuovi»[23]. Ora proprio la perimetrazione dello Stato digitale comporta non una sua difesa, perché lo Stato digitale incide su un "non luogo", ma un esercizio di una pubblica funzione derivata dalla sovranità statale[24].
Con l'art. 33 del d.lgs. 138/2024 gli obblighi di gestione del rischio per la sicurezza informatica e di notifica di incidente previsti dal d.l. 21 settembre 2019, n. 105, convertito, con modificazioni, dalla l. 18 novembre 2019, n. 133, sono considerati equivalenti a quelli previsti dal d.lgs. n. 138 del 2024. Inoltre, alle reti, ai sistemi informativi e ai servizi informatici inseriti nell'elenco di cui all'art. 1, c. 2, del d.l. 105/2019, non si applicano le disposizioni di cui allo stesso d.lgs. n. 138/2024, restando fermi gli obblighi per i sistemi informativi e di rete. Infine, i soggetti di cui all'art. 1, c. 2-*bis*, del d.l. 105/2019, non sono sottoposti agli obblighi di notifica per gli incidenti riconducibili a una notifica già effettuata per la specificità dell'attività. Pertanto, proprio come forma di esercizio della *public cybersecurity* dovremmo ritenere l'esercizio sul Perimetro Nazionale dell'esercizio delle competenze dell'Agenzia per la Cybersicurezza Nazionale.

4. L'Agenzia per la Cybersicurezza Nazionale e l'esercizio delle funzioni di vigilanza sul cyberspazio

Il d.lgs. 14 giugno 2021 n. 82 recante "Disposizioni urgenti in materia di cybersicurezza", ha ridefinito l'architettura nazionale di cybersicurezza e ha istituito l'Agenzia per la cybersicurezza nazionale, convertito con modificazioni dalla legge 4 agosto 2021 n. 109.

[23] Vedi L. Torchia, *Lo Stato,* cit., 19

[24] Vedi M. Luciani, voce *Integrazione europea, sovranità statale e sovranità popolare*, in *Treccani online*, 2009; R. Bin, *La sovranità nazionale e la sua erosione*, in R. Bifulco-O. Roselli, (a cura di), *Crisi economica e trasformazioni della dimensione giuridica. La costituzionalizzazione del pareggio di bilancio tra internazionalizzazione economica, processo di integrazione europea e sovranità nazionale*, Torino, 2013, 370 ss.; A. Vignudelli, *Diritto costituzionale*, Torino, 2019, 108 ss.; A. Pisaneschi, *Diritto Costituzionale*, Torino, 2016, 84 ss.

Esso appare disciplinare il settore della cybersicurezza in Italia, individuando competenze, soggetti e contenendo importanti novità, aspirando così ad essere il prodotto legislativo più completo e aggiornato in materia, anche in allineamento con il Piano nazionale di ripresa e resilienza (PNRR), di cui la sicurezza cibernetica costituisce uno degli interventi previsti[25]. La cybersicurezza costituisce infatti l'Investimento 1.5 - rimesso direttamente all'Agenzia per la cybersicurezza nazionale - della Missione 1 del PNRR - "Digitalizzazione, Innovazione, Competitività, Cultura e Turismo".

Da un punto di vista di qualificazione, a norma dell'art. 7 del d.lgs. 82/2021, l'Agenzia per la cybersicurezza nazionale costituisce l'autorità nazionale competente NIS e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi e Autorità nazionale di certificazione della cybersicurezza.

In quanto Autorità nazionale di cybersicurezza, l'ACN è chiamata ad assicurare, ferme le competenze di altre amministrazioni e le attribuzioni del Ministero dell'interno nella qualità di autorità nazionale di pubblica sicurezza, «il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale» e promuovere «la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore» (art. 7, c. 1, lett. a).

L'Agenzia come autorità nazionale competente NIS (e NIS 2) si sostituisce in una certa misura al Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio, cui il decreto-legge perimetro aveva assegnato tale ruolo[26]. La disciplina elimina il riferimento al SISR, spostando la competenza in capo all'Agenzia relativamente ai settori e sottosettori di cui all'allegato II e ai servizi di cui all'allegato III del d.lgs. NIS, con contestuale designazione delle autorità di settore (art. 15, c. 1 lett. g), che modifica l'art. 7 del d.lgs. c.d. NIS). Proprio nel raccordo tra autorità nazionale competente e autorità di settore, è stato istituito presso l'Agenzia un Comitato tecnico di raccordo, presieduto dall'Agenzia stessa e composto da rappresentanti delle amministrazioni statali individuate quali autorità di settore (art. 15, c. 8, lett. i).

Inoltre, l'Agenzia viene designata quale punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi (art. 15, c. 3), essendo così chiamata a svolgere una funzione di collegamento e raccordo al fine di garantire la cooperazione transfrontaliera tra l'autorità nazionale competente NIS con le rispettive autorità di altri Stati membri. Come autorità nazionale competente NIS e punto di contatto unico, l'Agenzia consulta e collabora con l'autorità di contrasto e con il Garante per la protezione dei dati personali (art. 15, c. 6) e diviene altresì competente all'accertamento delle violazioni e all'irrogazione delle sanzioni, sempre previste dal d.lgs. c.d. NIS.

Non solo, il d.lgs. 82/2021, alla lett. f) del c. 1 dell'art. 7 specifica che l'Agenzia assume in realtà tutte le funzioni che le disposizioni vigenti attribuiscono al Ministero dello sviluppo economico. Vi si comprendono, in primo luogo, le funzioni che il decre-

[25] Vedi S. Rossa, *Cybersicurezza e pubblica amministrazione,* Napoli, 2023, 62 ss.

[26] Vedi L. Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale,* in *Giorn. dir. amm.,* 6, 2021, 721 ss.; I. Forgione, *Il ruolo,* cit., 95 ss.

to-legge perimetro ha assegnato al Centro di valutazione e certificazione nazionale, il quale viene, dunque, trasferito presso l'Agenzia per la cybersicurezza nazionale (art. 7, c. 4). Secondo poi, le funzioni relative alla sicurezza e all'integrità delle comunicazioni elettroniche (art. 7, c. 1, lett. f), n. 2) e quelle riferite alla sicurezza delle reti e dei sistemi informativi di cui al d.l.gs NIS (art. 7, c. 1, lett. f), n. 3). Confermano ciò le modifiche testuali di sostituzione apportate al decreto legislativo NIS e al decreto-legge perimetro (artt. 15, c. 2, lett. a), art. 16, c. 6, lett. a), e c. 8 del d.lgs. 82/2021).
Il Ministero dello Sviluppo Economico rimane competente autorità del settore infrastrutture digitali e servizi digitali NIS (art. 15, c. 1, lett. g).
Da enfatizzare, tra le funzioni, la partecipazione dell'ACN nella gestione ed esercizio dei poteri speciali (*golden power*) di cui al d.lgs. 21/2012: infatti, l'art. 7, c. 1, lett. g) dispone la partecipazione dell'Agenzia, per tutti gli ambiti di competenza, al Gruppo di coordinamento di cui ai regolamenti attuativi previsti dall'art. 1, c. 8, del d.l. 21/2012.
Continuando sul tema delle funzioni che provengono da altri enti, amministrazioni o organismi e che sono state assegnate all'Agenzia meritano una menzione le lett. h), i) e m) del c. 1 dell'art. 7 d.lgs. 82/2021.
In primo luogo, l'Agenzia assume tutte le funzioni in materia di perimetro di sicurezza nazionale cibernetica che il decreto legge perimetro e successivi provvedimenti attuativi avevano rispettivamente attribuito alla Presidenza del Consiglio dei ministri (lett. h) - incluse le attività di ispezione e verifica *ex* art. 1, c. 6, lett. c) del decreto-legge perimetro e le funzioni relative all'accertamento delle violazioni e all'irrogazione delle sanzioni – al DIS (lett. i) e all'Agenzia per l'Italia digitale (AgID).
In particolare, quanto all'AgID si segnala che il c. 1, lett. m), dell'art. 7 del d.lgs. 82/2021, pone l'accento su alcune delle funzioni attualmente trasferite all'ACN: quelle di cui all'art. 51 del d.l.gs 82/2005 (c.d. Codice dell'amministrazione digitale) in materia di Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni[27]; le competenze *ex* art. 71 del d.lgs. 82/2005 relative all'adozione di linee guida contenenti regole tecniche di cybersicurezza e, infine, le competenze che l'AgID si vedeva assegnata dall'art. 33 *septies,* c. 4, del d.lgs. 179/2012, vale a dire quelle relative a stabilire livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione, nonché alla definizione delle caratteristiche di qualità, sicurezza, performance e scalabilità, interoperabilità, e portabilità dei servizi *cloud* per la pubblica amministrazione. Inoltre, sulla stessa linea - e rientrante in modo più specifico nell'ultimo capoverso dell'art. 33 *septies,* c. 4, del d.lgs. 179/2012 - la lettera m-*ter* dell'art. 7, c. 1, dispone che l'Agenzia «provvede alla qualificazione dei servizi *cloud* per la pubblica amministrazione», competenza prima appartenente all'AgID.
Relativamente alle funzioni che vengono trasferite dall'AgID all'Agenzia *ex* art. 7, c. 1, lett. m), il d.lgs. 82/2021 stabilisce che, per le funzioni che restano di competenza dell'AgID, i raccordi tra le due amministrazioni vengono definiti attraverso decreti del Presidente del Consiglio dei Ministri.
Si segnala, inoltre, che il CSIRT italiano, di cui al d.lgs. c.d. NIS, viene trasferito dalla Presidenza del Consiglio dei ministri all'Agenzia, assumendo la denominazione di

[27] Ancora L. Parona, *L'istituzione*, cit.

CSIRT Italia (art. 7, c. 3).
Inoltre, uno dei compiti più rilevanti che l'Agenzia ha in carico è la predisposizione della Strategia nazionale di cybersicurezza (art. 7, c. 1, lett. b) la quale viene approvata dal Presidente del Consiglio dei Ministri, sentito il Comitato Interministeriale per la Cybersicurezza. Recentemente è stata approvata e pubblicata la Strategia Nazionale di cybersicurezza 2022-2026 con relativo piano di implementazione, la quale si compone di tre obiettivi strategici: Protezione, Risposta e Sviluppo. Inoltre, l'ACN svolge attività di supporto al funzionamento del Nucleo per la cybersicurezza (art. 7, c. 1, lett. c) ed è chiamata allo sviluppo di capacità nazionali di prevenzione, monitoraggio, analisi e risposta, al fine di prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CSIRT Italia e con la possibilità di promuovere iniziative di partenariato pubblico-privato funzionali allo scopo (art. 7, c. 1, lett. n). In particolare, la gestione e mitigazione del rischio in materia di cybersicurezza appartengono all'Obiettivo Strategico "Risposta", che vede tra gli attori principali l'ACN, il Nucleo per la Cybersicurezza e il CSIRT Italia.
In aggiunta, l'ACN è incaricata di curare e promuovere «la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo conto anche degli orientamenti e degli sviluppi in ambito internazionale» ed esprimersi attraverso pareri non vincolanti sulle iniziative di leggi o regolamenti attinenti alla sicurezza cibernetica (art. 7, c. 1, lett. p)[28].
Da un punto di vista delle funzioni sostanziali non può non menzionarsi l'art. 7, c. 1 lettera m-*bis*, la quale dispone che l'Agenzia «assume le iniziative idonee a valorizzare la crittografia come strumento di cybersicurezza, anche attraverso un'apposita sezione dedicata nell'ambito della strategia di cui alla lettera b)».
La valorizzazione della crittografia viene spiegata, nella medesima disposizione, come parte di una generale attività dell'Agenzia rispetto ad «ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali».
Dal momento che la strategia è disponibile, è possibile verificare che la crittografia rientra nell'Obiettivo Strategico "Protezione" – al cui vertice è collocata l'ACN – i cui beneficiari sono individuati nelle istituzioni, negli operatori privati e nella società civile, dunque, la platea più ampia che la strategia stessa ammette. Altresì, la strategia specifica che la promozione dell'uso della crittografia "come strumento di cybersicurezza" si sostanzia nel favorire un impiego di questa – nella sua tipologia commerciale - lungo tutto il ciclo di vita di prodotti, sistemi e servizi ICT, essendo contestualmente esplicitata l'intenzione dell'Agenzia di sviluppare tecnologie e sistemi di cifratura nazionale.
Sul versante delle funzioni e ruoli dell'Agenzia a livello di cooperazione internazionale ed europea, l'art. 7 offre un quadro più che esteso[29]. Infatti, oltre che al già menzionato ruolo di autorità nazionale competente NIS punto di contatto unico, l'ACN è designata quale Centro nazionale di coordinamento ai sensi dell'art. 6 del regolamento (UE) 2021/887 che istituisce il Centro europeo di competenza per la cybersicurezza

[28] Ancora I. Forgione, *Il ruolo*, cit.

[29] Ci si permette di rinviare ai saggi contenuti in C. Cavaceppi-A. Contaldo (a cura di), *Cybersecurity*, cit.

nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento (art. 7, c. 1, lett. aa), il cui rappresentante nazionale (e sostituto) sono nominati con decreto del Presidente del Consiglio dei ministri.
Da un punto di vista funzionale, l'ACN è deputata a partecipare alle esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese (art. 7, c. 1, lett. o) e a coordinare, in raccordo con il Ministero degli Affari Esteri e della Cooperazione Internazionale, la cooperazione internazionale in materia di cybersicurezza. In aggiunta, l'Agenzia ha in carico la cura dei rapporti con organismi, istituzioni ed enti competenti e monitorare le tematiche di cybersicurezza, ferme le competenze che già sono attribuite dalla legge ad altre amministrazioni, con le quali comunque l'Agenzia è tenuta ad operare in raccordo per garantire l'uniformità e la coerenza delle posizioni nazionali con le politiche di cybersicurezza definite dal Presidente del Consiglio dei Ministri (art. 7, c. 1, lett. q). L'Agenzia può altresì stipulare accordi bilaterali e multilaterali, anche coinvolgendo il settore privato e industriale, con istituzioni, enti ed organismi di altri paesi (art. 7, c. 1, lett. s) ed è incaricata di garantire promozione, sostegno e coordinamento alla partecipazione italiana a progetti e iniziative dell'UE e internazionali nel campo della cybersicurezza (art. 7, c. 1, lett. t). Tali funzioni trovano tutte il proprio limite nelle competenze di altre amministrazioni, con cui l'ACN deve sempre assicurare il relativo raccordo, e del MAECI. Da sottolineare il rilievo dell'ultimo capoverso dell'art. 7, c. 1, lett. t), che specifica che la necessarietà del raccordo anche con il Ministero della Difesa per «per gli aspetti inerenti a progetti e iniziative in collaborazione con la NATO e con l'Agenzia Europea per la Difesa».

5. Brevi conclusioni: il cyberspazio come non luogo di intervento dello Stato per la funzione di "pubblica sicurezza digitale"

Il cyberspazio appare così come una sorta di non luogo di progettazione matematica in cui oramai si svolgono molte attività umane aventi anche rilevanza economica e finanziaria[30]. Lo Stato pertanto deve attivarsi per garantirvi soprattutto la funzione di Pubblica sicurezza nel cyberspazio[31], che in riferimento alle attività di governo statale e di livello centrale e locale necessitano di un complesso di apparati, autorità e strutture preposte alla tutela dell'ordine pubblico e all'incolumità delle persone. Tali soggetti sono preposti al fine di garantire un minimo grado di sicurezza per i cittadini di uno Stato, per fronteggiare emergenze e gravi necessità collettive, nell'obiettivo dell'incolumità pubblica, e per garantire l'ordine pubblico.
Il grado di sicurezza percepito dalla popolazione fornisce un notevole contributo alla stabilità economica e all'attrattività di un paese, alla produttività dei cittadini e in conclusione al successo economico di una nazione.
La pubblica sicurezza nel cyberspazio riguarda perciò tanto le attività di polizia, volte

[30] Ancora S. Pietropaoli, *Informatica*, cit. 81 ss.

[31] Vedi R. Ursi, *La sicurezza cibernetica come funzione pubblica*, in Idem (a cura di), *La sicurezza*, cit., 7 ss.

ad assicurare la "sicurezza" attraverso il rispetto delle norme di legge, quanto quelle comunque finalizzate a "prevenire" che la comunità possa patire danni da eventi fortuiti e accidentali, infortuni e disastri di qualunque altro genere[32], o comunque a prevenirne l'aggravio del danno, attraverso l'organizzazione di forme di prevenzione. Il costante espresso riferimento normativo, che si traduce in una frequente citazione della locuzione a fini amministrativi e burocratici, ha inoltre segnalato il pesante sbilanciamento ordinamentale verso una preminenza delle funzioni di polizia nelle attività di preservazione della pubblica sicurezza[33]. In particolare, gli interventi legislativi straordinari atti a potenziare le attività di pubblica sicurezza in materia di contrasto al terrorismo internazionale hanno posto l'accento sullo sviluppo delle capacità di indagine e prevenzione e sull'aumento e la diversificazione delle forze in campo, ma sono riuscite solo marginalmente nel compito di migliorare il coordinamento degli organi di pubblica sicurezza nazionali.

[32] *Ibid.*

[33] Vedi P. Vipiana, *Introduzione*, cit., 131 ss.; R. Ursi, *La sicurezza pubblica*, cit., 182 ss.

Note a sentenza

Sull'acquisizione da parte della polizia giudiziaria delle chat dell'indagato mediante screenshot: ancora un passo avanti della Cassazione nella tutela della riservatezza delle comunicazioni e delle garanzie difensive*

Sara Mastrapasqua

Corte di cassazione, sez. VI penale, 20 novembre 2024 (dep. 13 gennaio 2025), n. 1269

In tema di acquisizione della messaggistica istantanea mediante screenshot, la polizia giudiziaria ha il dovere di procedere al sequestro del telefono senza poter accedere al suo contenuto, prima di ottenere una formale autorizzazione da parte del pubblico ministero, anche se l'indagato abbia fornito il proprio consenso dopo l'avviso della facoltà di farsi assistere da un difensore.

Sommario

Keywords

Cassazione - messaggistica WhatsApp – screenshot – sequestro di corrispondenza -garanzie

*Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

1. Introduzione

Con la sentenza in commento la Corte di cassazione si è pronunciata sul tema della acquisizione mediante screenshot delle chat archiviate nello smartphone dell'indagato, segnando un ulteriore passo avanti nella tutela della riservatezza delle comunicazioni e delle correlate garanzie difensive. Trattasi di un tema di sicura attualità e rilevanza nel nostro sistema, in ragione dell'uso sempre più frequente e diffuso della messaggistica istantanea, nonché del significativo contributo che essa può fornire all'accertamento processuale penale. L'intervento dei giudici di legittimità riveste particolare interesse, poiché pone forti limiti all'attività di acquisizione della polizia giudiziaria, riconoscendo l'importanza di assicurare adeguate tutele all'indagato durante lo svolgimento degli atti investigativi.

2. Il caso

Il caso sottoposto all'attenzione della Corte concerne un imputato condannato per il reato di cui agli artt. 81 c.p. e 73, c. 5, T.U. Stup., con sentenza emessa all'esito di giudizio abbreviato dal Giudice per le indagini preliminari del Tribunale di Taranto. La pena inflitta è stata ridotta dalla Corte di appello di Lecce, sezione distaccata di Taranto, a un anno e sei mesi di reclusione ed euro 1.800,00 di multa.
Tra gli elementi valorizzati ai fini della condanna, vi era il possesso di trenta dosi di sostanza stupefacente del tipo cocaina, suddivisa in più involucri, il rinvenimento sulla persona dell'indagato di banconote di piccolo taglio "accartocciate", nonché l'assenza di redditi da lavoro compatibili con le disponibilità economiche necessarie per l'acquisto di una cospicua provvista di sostanza stupefacente. Inoltre, il G.i.p. aveva ritenuto utilizzabili i contenuti di talune chat WhatsApp estratte dal telefono dello stesso imputato, mediante un rilievo fotografico (c.d. screenshot) operato dalla polizia giudiziaria dopo il rinvenimento della sostanza stupefacente nascosta dall'indagato sulla sua persona. Nello specifico, la polizia giudiziaria aveva ottenuto il consenso ad accedere allo smartphone dell'imputato tramite la password fornita dallo stesso nel corso della perquisizione e del conseguente sequestro della sostanza stupefacente, senza avvisarlo della facoltà di farsi assistere da un difensore, oltre che del diritto di non prestare il consenso a tale accesso.
L'imputato, tramite il proprio difensore di fiducia, proponeva ricorso per cassazione, lamentando, tra le altre cose e per quanto qui di interesse, l'inutilizzabilità c.d. patologica degli screenshot delle chat estratte dal proprio telefono cellulare, in quanto acquisite con modalità illegittime, in violazione dei diritti di difesa, pure a seguito di perquisizione e conseguente sequestro anch'essi, a suo dire, illegittimi per omissione dell'avviso della facoltà di farsi assistere da un difensore. Rappresentava, inoltre, la decisività di tali elementi di prova per l'accertamento della destinazione allo spaccio della sostanza stupefacente sequestrata e chiedeva, di conseguenza, l'annullamento della condanna.

3. La decisione della Corte di cassazione

La Corte ha rigettato il ricorso, ritenendolo nel suo complesso infondato. Tuttavia, ha ritenuto fondate le questioni eccepite dal ricorrente in relazione alla inutilizzabilità delle chat estrapolate dal telefono in suo possesso, pur considerando il motivo di ricorso non meritevole di accoglimento, sotto il profilo della c.d. prova di resistenza. A tal proposito, i giudici di legittimità hanno ricordato il consolidato principio in base al quale qualora con il ricorso per cassazione si lamenti l'inutilizzabilità di un elemento a carico, «il motivo di impugnazione deve illustrare, a pena di inammissibilità per aspecificità, l'incidenza dell'eventuale eliminazione del predetto elemento ai fini della cosiddetta "prova di resistenza", in quanto gli elementi di prova acquisiti illegittimamente diventano irrilevanti ed ininfluenti se, nonostante la loro espunzione, le residue risultanze risultino sufficienti a giustificare l'identico convincimento»[1]. Nel caso di specie, la prova della destinazione della sostanza stupefacente allo spaccio emergeva comunque dalle altre risultanze legittimamente acquisite ai fini della decisione, come già rilevato nella sentenza dal giudice di primo grado; nessuna giustificazione del possesso della sostanza stupefacente è stata peraltro fornita dall'imputato nel corso del giudizio. A parere della Corte, anche la perquisizione e il conseguente sequestro della sostanza sono da ritenersi legittimi, benché la perquisizione non sia stata preceduta dall'avviso del diritto ad essere assistito da un difensore. Sul punto, la Suprema Corte ricorda, richiamando alcuni precedenti[2], che la perquisizione per la ricerca di sostanze stupefacenti ai sensi dell'art. 103 T.U. Stup. ha carattere speciale rispetto alla disciplina generale dei mezzi di ricerca della prova: poiché essa non presuppone l'esistenza di una notizia di reato, non occorre la preventiva autorizzazione dell'autorità giudiziaria, né che la persona sottoposta a controllo sia avvisata del diritto all'assistenza di un difensore. Minori garanzie si giustificano sulla base dell'esigenza di contrastare talune forme di criminalità, che rende opportuna «l'attribuzione alla polizia giudiziaria di poteri più ampi rispetto a quelli codificati»[3]. Ad ogni modo, osservano i giudici di legittimità, il sequestro del corpo del reato, quale la sostanza stupefacente rinvenuta in possesso dell'imputato, è da ritenersi legittimo «perché, costituendo un atto dovuto, rende del tutto irrilevante il modo con cui ad esso sia pervenuti»[4].

3.1 La nozione di corrispondenza

Fatte queste brevi premesse, la Corte di cassazione passa ad esaminare la questione dedotta con riferimento all'inutilizzabilità delle chat, fornendo un chiaro contributo su un tema recentemente molto dibattuto. In primo luogo, richiama la recente sentenza

[1] Cfr. par. 1 delle considerazioni in diritto.

[2] Il riferimento è a Cass. pen., sez. III, 9 febbraio 2011, n. 8097, *CED* 249545; Cass. pen., sez. III, 17 febbraio 2016, n. 19365, *CED* 266580.

[3] Così Corte cost., 21 ottobre 2020, n. 252, richiamata dalla pronuncia in esame.

[4] Così Cass. pen., sez. un., 27 marzo 1996, n. 5021, imp. Suraci, *CED* 204643.

della Corte costituzionale n. 170/2023[5], ritenendo i principi da essa sanciti applicabili anche nel caso di specie. Come si ricorderà, con tale pronuncia la Consulta ha esteso le garanzie di salvaguardia del diritto alla riservatezza dei dati archiviati sulla memoria di un telefono cellulare, attraverso il riconoscimento della natura di corrispondenza anche alle comunicazioni non più *in itinere* ma acquisite dopo la ricezione da parte del destinatario. In particolare, si è osservato come in tale nozione debbano ricomprendersi altresì i messaggi WhatsApp, anche dopo che siano stati ricevuti e letti, qualora conservati nella memoria del dispositivo elettronico del destinatario o del mittente. Del resto, «quello di "corrispondenza" è concetto ampiamente comprensivo, atto ad abbracciare ogni comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate, attuata in modo diverso dalla conversazione in presenza»[6]. Ne consegue che la garanzia di cui all'art. 15 Cost., che tutela la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, consentendone la limitazione soltanto per atto motivato dell'autorità giudiziaria, si estende «a ogni strumento che l'evoluzione tecnologica mette a disposizione a fini educativi, compresi quelli elettronici e informatici» e rimane valida anche dopo che la comunicazione è giunta a conoscenza del destinatario, finché conservi carattere di attualità. La menzionata pronuncia rappresenta un'indubbia svolta in materia, dal momento che ha fornito un'interpretazione del concetto di "corrispondenza" certamente più adeguata all'impatto delle tecnologie sulla vita individuale e collettiva della persona[7]. Vale la pena ricordare infatti che prima dell'intervento della Corte costituzionale, la giurisprudenza della Corte di cassazione riteneva, in termini opposti, in misura pressoché unanime, che i messaggi Whatsapp e gli sms conservati nella memoria di un telefono cellulare dovessero essere considerati documenti ai sensi dell'art. 234 c.p.p. o, al più, documenti informatici con conseguente applicazione dell'art. 234-*bis* c.p.p. e che, dunque, non rientrassero nel concetto di "corrispondenza", «implicando tale nozione un'attività di spedizione in corso o comunque avviata al mittente mediante la consegna del plico a terzi per il recapito»[8]. Si escludeva, dunque, che per la loro acquisizione dovessero applicarsi sia le disposizioni in materia di intercettazioni, le quali esigono la captazione di un flusso di comunicazioni in atto, sia quelle relative al sequestro di corrispondenza, proprio in considerazione della impossibilità di ritenere tale

[5] Corte cost., 7 giugno 2023, n. 170, con nota di P. Villaschi, *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*, in questa *Rivista*, 2, 2023.

[6] Cfr., nuovamente, Corte cost., 7 giugno 2023, n. 170.

[7] In questi termini, G. M. Baccari, *La Corte costituzionale torna a pronunciarsi sull'acquisizione dei messaggi WhatsApp*, in *Processo penale e giustizia*, 4, 2024, 880. Si ricordi che i principi sanciti dalla menzionata sentenza della Corte costituzionale sono stati poi ribaditi dalla successiva sentenza n. 227 del 28 dicembre 2023 e che a distanza di meno di un anno la giurisprudenza costituzionale è stata richiamata dalle due sentenze "gemelle" delle Sezioni Unite della Cassazione del 29 febbraio 2024 (n. 23755, imp. Gjuzi Ermal, *CED* 286573, e n. 23756, imp. Giorgi, *CED* 286589), che hanno fatto propria la definizione di "corrispondenza" fornita dalla Consulta anche con riguardo ai messaggi WhatsApp conservati nella memoria dei dispositivi mobili.

[8] Cass. pen., sez. III, 25 novembre 2015, n. 928, *CED* 265991; negli stessi termini v. anche, più recentemente, Cass. pen., sez. VI, 21 settembre 2023, n. 38678, con nota di M. Cecchi, *Ancora una pronuncia di legittimità sull'utilizzabilità, come prova documentale, dei messaggi estrapolati da dispositivi mobili*, in *Penale Diritto e Procedura*, 2023.

materiale rientrante nella nozione di corrispondenza[9]. Peraltro, tali principi sono stati applicati anche dalle Sezioni Unite civili della Cassazione che, ai fini dell'accertamento dei fatti nell'ambito di procedimenti disciplinari a carico di magistrati, hanno sancito la legittimità dell'acquisizione di messaggi WhatsApp conservati nella memoria di un telefono cellulare mediante mera riproduzione fotografica (screenshot), anche da parte della polizia giudiziaria.
Diversamente, a parere della Consulta, ai fini del riconoscimento delle garanzie previste dall'art. 15 Cost., ciò che rileva è la natura comunicativa del contenuto e non le tecniche di acquisizione dello stesso, che possono essere diverse a seconda delle modalità con le quali viene trasmesso e rinvenuto[10]. La Corte di cassazione, nella pronuncia in commento, rileva come, in virtù di queste considerazioni, «anche la messaggistica archiviata nei telefoni cellulari non può più essere considerata alla stregua di un mero documento, liberamente acquisibile senza la garanzia costituzionale prevista dall'art. 15 Cost., ma richiede l'assoggettamento alla disciplina dell'art. 254 cod. proc. pen. che impone la necessità di un provvedimento dell'autorità giudiziaria, necessariamente motivato al fine di giustificare il sacrificio della segretezza della corrispondenza»[11]. Pertanto, è da escludersi la «possibilità di accesso diretto» da parte della polizia giudiziaria, alla quale è riconosciuto il solo potere di «acquisire materialmente il dispositivo elettronico ma senza accesso diretto al suo contenuto, analogamente a quanto previsto per l'invio della corrispondenza postale dall'art. 254, comma 2, cod. proc. pen., e fermo quanto disposto dall'art. 353 cod. proc. pen. sull'apertura dei plichi o di corrispondenza con l'autorizzazione del pubblico ministero quando ciò sia necessario per l'assicurazione di elementi di prova che potrebbero andare persi a causa del ritardo».

3.2 I limiti all'acquisizione delle chat

Con riguardo ancora alla censura della inutilizzabilità delle chat estratte dalla polizia giudiziaria, ulteriore questione su cui la Corte si è pronunciata riguarda il ruolo del consenso dell'indagato all'acquisizione degli screenshot dal proprio telefono cellulare. Ci si interroga, in particolare, se il consenso, pur liberamente prestato dall'indagato, possa ritenersi sufficiente per l'accesso (da parte della polizia giudiziaria) ai contenuti del telefono, in assenza di un provvedimento emesso dall'autorità giudiziaria, di autorizzazione preventiva o di convalida successiva all'atto di indagine posto in essere in totale autonomia dalla polizia giudiziaria. A tal proposito, i giudici di legittimità osservano innanzitutto che ove l'attività sia svolta, come nel caso di specie, nei confronti di un soggetto, già gravato da elementi indiziari tali da giustificare l'acquisizione della posizione di indagato[12], ogni ulteriore atto di indagine che richieda la collaborazione

[9] Cfr. G. M. Baccari, *La Corte costituzionale torna a pronunciarsi sull'acquisizione dei messaggi WhatsApp*, cit., 881.

[10] A. Nocera, *L'acquisizione delle chat whatsapp e messenger: intercettazione, perquisizione o sequestro?*, in *Il penalista*, 2018.

[11] Cfr. par. 3 delle considerazioni in diritto.

[12] Nel caso di specie, la richiesta di accesso ai contenuti del telefono era infatti avvenuta soltanto dopo

della persona indagata deve essere espletato «dopo la formale comunicazione degli avvisi di tutte le facoltà difensive ad essa spettanti, ivi compresa quella della facoltà di rifiutare tale collaborazione ed il diritto ad essere assistito da un difensore, espressamente previsto dal combinato disposto degli artt. 356 cod. proc. pen. e 114 disp. att. cod. proc. pen. non solo per le perquisizioni e sequestri (art. 352 e 354, stesso codice), ma anche per l'apertura della corrispondenza (ex art. 353 cod. proc. pen.)». Inoltre, la Corte rileva che già il giudice di primo grado aveva escluso la possibilità di qualificare come spontanee le dichiarazioni confessorie rese dall'indagato nel medesimo contesto, proprio sulla scorta del condivisibile orientamento della giurisprudenza di legittimità che sancisce l'assoluta inutilizzabilità, anche pro reo, se non ai soli fini della immediata prosecuzione delle indagini secondo quanto previsto dall'art. 350, commi 5 e 6, c.p.p., delle dichiarazioni rese dall'indagato nell'immediatezza dei fatti su "sollecitazione" dalla polizia giudiziaria, in assenza del «previo avviso circa la facoltà di esercitare il diritto al silenzio» e della «presenza del difensore»[13].
In secondo luogo, i giudici di legittimità affermano che il consenso dell'indagato, anche se fosse stato reso dopo l'avviso della facoltà di farsi assistere da un difensore, non avrebbe comunque potuto supplire alla carenza di un provvedimento emesso dall'autorità giudiziaria: resta, infatti, «imprescindibile, onde prevenire il rischio di abusi, che in situazioni del genere la polizia giudiziaria abbia il dovere di procedere al sequestro del telefono senza poter accedere al suo contenuto, prima di una formale autorizzazione da parte del pubblico ministero, in applicazione della disciplina processuale […] relativa all'apertura della corrispondenza (vedi art. 353 cod. proc. pen.)».

3.3 Esclusione dell'atipicità probatoria

Da ultimo, la Cassazione critica la ricostruzione fornita nel giudizio di merito dalla Corte d'appello, secondo cui l'acquisizione dei contenuti delle chat sarebbe avvenuta attraverso un'attività di acquisizione alternativa da parte della polizia giudiziaria, qualificabile come «legittima assunzione di una prova atipica». A parere dei giudici di legittimità, non può giungersi a tale conclusione, in quanto contrastante con il principio, già affermato in precedenza dalla medesima Corte[14], secondo il quale «non è consentito alla polizia giudiziaria, in un sistema rigorosamente ispirato al principio di legalità, scostarsi dalle previsioni legislative per compiere atti atipici i quali, permettendo di conseguire risultati identici o analoghi a quelli conseguibili con gli atti tipici, eludano tuttavia le garanzie costituzionali dettate dalla legge per questi ultimi». Per comprendere questo approccio, occorre ricordare che la polizia giudiziaria, ai sensi dell'art. 348 c.p.p., è abilitata a compiere attività di indagine tipica[15], ma anche atti investigativi

il rinvenimento della sostanza stupefacente nascosta dall'indagato sulla sua persona.

13 Cass. pen., sez. II, 12 gennaio 2017, n. 3930, *CED* 269260.

14 Cass. pen., sez. VI, 24 febbraio 2003, n. 13623, *CED* 224741.

15 V. art. 348, c. 2, lett. c), c.p.p., secondo cui la polizia giudiziaria procede «tra l'altro» «al compimento degli atti indicati negli articoli seguenti», vale a dire attività identificative (art. 349 c.p.p.), sommarie informazioni (artt. 350 e 351 c.p.p.), perquisizioni (art. 352 c.p.p.), acquisizioni di plichi e corrispondenza

atipici, dovendo raccogliere «ogni elemento utile alla ricostruzione del fatto e alla individuazione del colpevole» (art. 348, c. 1, c.p.p.). Precisamente, l'atipicità investigativa trova fondamento nelle disposizioni del Libro V del codice di rito, che attribuiscono al pubblico ministero e alla polizia giudiziaria il potere di svolgere, nell'ambito delle rispettive attribuzioni, «le indagini necessarie per le determinazioni inerenti all'esercizio dell'azione penale» (art. 326 c.p.p.)[16]. Come è noto, sono però previsti specifici limiti, a pena di inutilizzabilità della prova, alle operazioni atipiche, i quali sono tracciati dai profili di tassatività del catalogo legale dei mezzi investigativi; restano inoltre fermi i criteri di cui all'art. 189 c.p.p. nonché il rispetto dei diritti fondamentali dell'indagato, la cui limitazione è consentita solo nei casi e nei modi previsti dalla legge e con atto motivato dell'autorità giudiziaria (art. 13 Cost.). Ed ecco che un profilo di tassatività del catalogo dei mezzi di ricerca della prova è rinvenibile proprio nella disciplina relativa all'acquisizione di plichi o di corrispondenza di cui all'art. 353 c.p.p., la cui applicazione è richiamata dalla Corte nel caso di specie per affermare il dovere della polizia giudiziaria di procedere al sequestro del telefono senza accedere al suo contenuto, prima di una formale autorizzazione del pubblico ministero[17]. Tale norma garantisce, del resto, la libertà e la segretezza delle comunicazioni, prevedendo modalità assuntive tipiche della prova che non lasciano spazio a deroghe. Nello specifico, essa sancisce il dovere della polizia giudiziaria di a) procedere al sequestro senza prendere conoscenza del contenuto; b) procedere al sequestro e, soltanto a seguito di autorizzazione del p.m., accedere al contenuto, previo avviso all'indagato della facoltà di farsi assistere da un difensore, a pena di nullità *ex* art. 178 c.p.p.

4. Osservazioni conclusive

La pronuncia in commento, come si anticipava, ha evidentemente il merito di porre dei significativi limiti all'attività svolta dalla polizia giudiziaria nei confronti di persona sottoposta alle indagini, operando un bilanciamento tra esigenze di acquisizione della prova e garanzie di riservatezza *ex* art. 15 Cost. L'orientamento della Corte di cassazione appare coerente non solo con la più recente giurisprudenza costituzionale, ma anche con i principi sanciti dalla Corte di giustizia dell'Unione europea che, pronunciatasi in tema di accesso ai dati contenuti in un telefono cellulare, ha precisato proprio la necessità dell'autorizzazione dell'autorità giudiziaria e la conseguente inutilizzabilità degli screenshot della messaggistica contenuta nel dispositivo eseguiti dagli agenti di polizia[18]. Peraltro, i giudici di legittimità operano un ulteriore passo avanti anche rispet-

(art. 353 c.p.p.), accertamenti urgenti e sequestro (art. 354 c.p.p.).

[16] In questi termini, M. Bontempelli, *Le indagini preliminari*, in Aa. Vv., *Procedura penale*, Torino, 2023, 499 ss.

[17] Cfr. par. 3 delle considerazioni in diritto.

[18] Il riferimento è a CGUE (Grande Camera), C-548/21, *Tribunale amministrativo regionale del Tirolo (Austria) c. Bezirkshauptmannschaft Landeck* (2024), in *Archivio Penale (Web)*, che ha precisato le condizioni in presenza delle quali le autorità nazionali competenti possono accedere ai dati contenuti in un telefono cellulare per finalità di prevenzione, indagine, accertamento e perseguimento dei reati in generale, con riferimento alla Direttiva n. 2016/680.

to a quanto osservato in un recente precedente con il quale, in presenza di una fattispecie analoga, con un *iter* motivazionale sviluppatosi secondo i già richiamati principi affermati dalla Corte costituzionale con la sentenza n. 170/2023, avevano ritenuto fondata l'eccezione di inutilizzabilità patologica sollevata dal ricorrente, in ragione della loro natura di corrispondenza, dei messaggi WhatsApp acquisiti mediante screenshot dal telefono cellulare dell'indagato, eseguiti dalla polizia giudiziaria di propria iniziativa e senza ragioni di urgenza, in assenza di decreto di sequestro del pubblico ministero[19]. Difatti, nella sentenza in esame la Cassazione ha affermato che neppure il consenso del titolare del dispositivo, già gravato da elementi indiziari tali da giustificare l'acquisizione della qualità di persona sottoposta alle indagini, anche qualora sia stato prestato liberamente e dopo l'avviso della facoltà di essere assistito da un difensore (che peraltro, come si è detto, è stato omesso nel caso di specie), può supplire alla carenza di un provvedimento dell'autorità giudiziaria. Diversamente, in simili ipotesi, ove si debbano acquisire i contenuti delle chat archiviate nel telefono dell'indagato, la polizia giudiziaria, in applicazione della disciplina processuale relativa all'apertura di corrispondenza, ha il dovere di procedere al sequestro del telefono senza accedere al suo contenuto, prima di una formale autorizzazione da parte del pubblico ministero. Del resto, è noto che, sebbene i messaggi conservati all'interno dei dispositivi mobili costituiscano sicuramente uno strumento di notevole valore per la ricostruzione dei fatti nella prospettiva processuale penale, l'accesso incontrollato ai contenuti di un telefono cellulare costituisce un'«ingerenza grave»[20] nei diritti fondamentali della persona interessata e deve essere, pertanto, tutelato attraverso il riconoscimento di adeguate garanzie.

È opportuno, infine, mettere in luce un ultimo aspetto, già in più occasioni evidenziato in dottrina, su cui tuttavia la pronuncia non si è soffermata, relativo ai problemi probatori che discendono dall'acquisizione nel processo penale di screenshot delle chat in assenza del sequestro del dispositivo fisico. È noto, del resto, come, in mancanza del dispositivo-contenitore, la riproduzione fotografica di uno screenshot o di un messaggio WhatsApp non assicuri con certezza l'identità del mittente, del destinatario, né tantomeno del contenuto del messaggio, integrando una prova di dubbia attendibilità in quanto facilmente suscettibile di alterazioni[21]. Eppure, dal riconoscimento della natura di prova documentale della messaggistica WhatsApp la giurisprudenza di legittimità faceva discendere l'utilizzabilità dei contenuti così acquisiti, anche in assenza del sequestro dell'apparecchio dal quale sono stati estratti[22]; la corrispondenza all'originale era asseverata dalla qualifica soggettiva dell'agente che effettuava la riproduzione[23]. Tale orientamento appare invero difficilmente condivisibile e si auspica che la pronuncia in commento ne segni il definitivo superamento.

---

[19] Cass. pen., sez. VI, 11 settembre 2024, n. 39548, in *Processo Penale e Giustizia*.

[20] Cfr. CGUE, C-548/21, cit.

[21] In questi termini, V. Filippi, *Acquisizione di screenshot consegnato alla polizia giudiziaria: è un documento?*, in *Penale Diritto e Procedura*, 2023; A. Vele, *Aspetti critici del documento probatorio "screenshot" e acquisito mediante il captatore informatico*, in *Archivio penale (Web)*, 1, 2024; R. Del Coco, *L'utilizzo probatorio dei dati whatsapp tra lacune normative e avanguardie giurisprudenziali*, in *Processo Penale e Giustizia*, 3, 2018.

[22] Cass. pen., sez. II, 1° luglio 2022, n. 39529, in *De Jure*.

[23] Cass. pen., sez. I, 20 febbraio 2019, n. 21731, *CED* 275895.

Da ultimo, è bene rammentare che ancora oggi bisogna fare i conti con il difetto di una disciplina specifica che regolamenti i presupposti dell'acquisizione dei contenuti dei dispositivi elettronici. Come è noto, lo scorso 11 aprile è stata trasmessa alla Camera la proposta di legge, approvata dal Senato, recante "Modifiche al codice di procedura penale in materia di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali". Essa prevede l'introduzione dell'art. 254-*ter* c.p.p., rubricato "Sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute", il quale, sulla scia della recente giurisprudenza in materia, si propone di attribuire al Giudice per le indagini preliminari il potere di disporre il sequestro dei supporti informatici, su richiesta del pubblico ministero, o il potere di convalida del sequestro disposto dal pubblico ministero o dalla polizia giudiziaria, su richiesta dello stesso pubblico ministero, nei casi d'urgenza, sancendo espressamente l'inutilizzabilità di tutte le acquisizioni che non rispettino le formalità prescritte. Senza addentrarsi in un'analisi della proposta di riforma[24] e nell'attesa di conoscere l'esito dell'*iter* legislativo, la disamina della pronuncia ci offre una nuova occasione per ribadire che soltanto una regolamentazione accurata della materia potrebbe – si spera – porre definitivamente fine a simili abusi.

[24] In argomento, si rinvia, *ex multis*, a S. De Flammineis, *Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale*, in *Sistema penale*, 2024; L. Tombelli, *La tutela della corrispondenza tra atipicità della prova e tentativi di riforma*, in *Penale Diritto e Procedura*, 2025.

La Corte di cassazione sulla competenza territoriale in caso di diffamazione a mezzo radiotelevisivo aggravata dall'attribuzione di un fatto determinato: il limite del dato normativo e il ritorno al giudice naturale*

Alessandro Nascimbeni

Corte di cassazione, sez. V penale, 15 marzo 2024, n. 26919
Corte di cassazione, sez. V penale, 14 giugno 2024, n. 34507
Corte di cassazione, sez. V penale, 10 ottobre 2024, n. 41956

In tema di diffamazione commessa attraverso trasmissioni televisive e consistente nell'attribuzione di un fatto determinato, la competenza territoriale deve essere stabilita, anche successivamente alla sentenza n. 150 del 2021 della Corte costituzionale, applicando l'art. 30, c. 5, legge 6 agosto 1990, n. 223, nel luogo di residenza della persona offesa, chiunque sia il soggetto chiamato a rispondere del reato.

Corte di cassazione, sez. V penale, 10 ottobre 2024, n. 41956

In caso di più delitti di diffamazione, commessi con un'unica azione attraverso l'impiego del mezzo radiotelevisivo e aggravati dall'attribuzione di un fatto determinato, la competenza territoriale per connessione deve essere determinata secondo il criterio suppletivo previsto dall'art. 9, c. 1, c.p.p.

Sommario

*Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

concorso formale omogeneo di reati. – 6. Rilievi conclusivi.

Keywords

diffamazione – competenza per territorio – competenza per connessione – giudice naturale – rinvio pregiudiziale

1. Il dato normativo e la pronuncia della Corte costituzionale n. 42 del 1996

Il c. 5 dell'art. 30 l. 223 del 1990[1] stabilisce che, in caso di diffamazione aggravata dall'attribuzione di un fatto determinato commessa col mezzo della radio o della televisione, la competenza territoriale appartiene al giudice del luogo di residenza della persona offesa. Si tratta di una delle «regole extravaganti»[2] al criterio generale di cui all'art. 8, c. 1, c.p.p. che trova invece applicazione nel caso di diffamazione mediatica[3] semplice.

Com'è noto, tale disciplina derogatoria[4] e, in particolare, la differenza di trattamento tra le due ipotesi di diffamazione (aggravata e semplice) era stata sottoposta al vaglio della Corte costituzionale, con riferimento al parametro di cui all'art. 3 Cost., già nel 1996[5]. In tale occasione, il Giudice delle leggi aveva individuato la *ratio* della «norma eccezionale»[6] nell'esigenza, particolarmente pressante nel caso di diffamazione mediatica aggravata, di attenuare lo squilibrio di posizioni tra chi commette il reato e chi del reato ne subisce le conseguenze lesive. Del tutto legittima, quindi, la scelta di radicare la competenza nel luogo di residenza della persona offesa al fine di permettere a quest'ultima di attivarsi a difesa della propria reputazione con un minore dispendio di tempo e di risorse economiche, peraltro avanti ad un giudice più idoneo al giudizio in quanto vicino al luogo di svolgimento dei fatti. Senza considerare, poi, la maggior efficacia riparatoria derivante dalla diffusione della sentenza nell'ambiente sociale normalmente frequentato dalla persona offesa.

Con la medesima pronuncia, la Corte costituzionale aveva inoltre respinto la que-

[1] L. 6 agosto 1990, n. 223: «Disciplina del sistema radiotelevisivo pubblico e privato», in *G.U.* 9 agosto 1990, n. 185, Suppl. ord. n. 53 (c.d. legge Mammì).

[2] Così F. Cordero, *Procedura penale*, Milano, 2012, 142 ss.

[3] Nel presente contributo si utilizzerà la locuzione "diffamazione mediatica" per riferirsi, esclusivamente, alla diffamazione commessa col mezzo radiotelevisivo.

[4] Numerose sono le deroghe alla regola del *locus commissi delicti* che traggono legittimazione dall'art. 210 disp. att. c.p.p.

[5] Corte cost., 23 febbraio 1996, sent. n. 42, in *Giur. cost.*, 1996, 330 ss. e in *Dir. pen. e proc.*, n. 7, 1996, 823 ss., con nota di L. Fioravanti.

[6] Secondo G. Corrias Lucente, *Prime osservazioni sugli aspetti penali della legge di disciplina del sistema radiotelevisivo*, in *Dir. inf. e infor.*, n. 2, 1991, 432, si tratta di «[n]orma eccezionale, dunque, ancora prima che speciale, in quanto disciplina in modo del tutto inusitato la competenza territoriale, privilegiando un criterio che non è previsto nemmeno fra quelli indicati come residuali dal codice di procedura penale (vecchio e nuovo)».

stione di legittimità sollevata con riferimento all'art. 25, c. 1, Cost.[7] ritenendo che dal principio di precostituzione del giudice naturale non discendesse alcun vincolo di collegamento tra il giudice ed il luogo di consumazione del reato[8]. Per la Corte, quindi, l'individuazione del giudice naturale è affidata alla discrezionalità del legislatore, libero di adottare criteri di competenza derogatori rispetto alle regole generali secondo una valutazione comunque razionale dei diversi interessi in gioco nel processo[9]. Del tutto legittima, in quest'ottica, una disciplina come quella prevista dall'art. 30, c. 5, l. 223 del 1990 che va a individuare, preventivamente e non in vista di singole controversie, il foro territorialmente competente nella residenza della persona offesa[10].

2. (segue): la questione interpretativa

Pur uscita indenne dal giudizio di costituzionalità, l'infelice formulazione[11] dell'art. 30 l. 223 del 1990 ha dato vita ad un contrasto giurisprudenziale in seno alla Corte di cassazione. Pomo della discordia l'ambito di applicazione della regola derogatoria in materia di competenza territoriale: esclusivamente ai soggetti imputati specificamente indicati al primo comma della disposizione (il concessionario privato, il concessionario

[7] Il giudice rimettente aveva ipotizzato la violazione dell'art. 25 Cost. poiché il principio del giudice naturale precostituito per legge impone di collegare "in qualche modo" la competenza territoriale al luogo di commissione del reato, evenienza preclusa alla luce dell'art. 30, c. 5, l. 223 del 1990 in tutte le ipotesi in cui esso non coincida con la residenza della persona offesa. Sul punto si veda G. Corrias Lucente, *Prime osservazioni sugli aspetti penali della legge di disciplina del sistema radiotelevisivo*, cit., 432, secondo il quale la determinazione della competenza territoriale operata da tale previsione segna «una differenza di trattamento che si riflette sulla posizione dell'imputato del reato di diffamazione, per il quale la competenza e la scelta del giudice è guidata da un fattore esterno alla condotta ed alla fattispecie: la residenza della persona offesa».

[8] Nella giurisprudenza costituzionale la "naturalità" di cui all'art. 25, c. 1, Cost. non ha mai goduto di autonoma considerazione rispetto al concetto di "precostituzione". In tal senso si veda, tra le altre, Corte cost., 1° aprile 1958, sent. n. 29, in *Giur. cost.*, 1958, 124 ss.; Corte cost., 3 luglio 1962, sent. n. 88, ivi, 1962, 966 ss., secondo cui «la locuzione giudice naturale, come sostanzialmente questa Corte ha ritenuto anche in precedente sentenza (n. 29 del 1958), non ha nell'art. 25 un significato proprio e distinto, e deriva per forza di tradizione da norme analoghe di precedenti Costituzioni, nulla in realtà aggiungendo al concetto di giudice precostituito per legge»; Corte cost., 13 giugno 1995, ord. n. 257, ivi, 1995, 1874 ss.; Corte cost., 1° aprile 2009, ord. n. 102, ivi, 2009, 921 ss.: «l'ordinamento costituzionale non propone una nozione autonoma di giudice naturale […] da quella di giudice precostituito […] sicché giudice naturale è quello prefigurato dalla legge, secondo criteri generali che, nei limiti della non manifesta irragionevolezza e arbitrarietà, appartengono alla discrezionalità legislativa».

[9] Cfr. Corte cost., 26 ottobre 1989, ord. n. 508, in *Giur. cost.*, 1989, 2362 ss.; Corte cost., 5 dicembre 1974, sent. n. 274, ivi, 1974, 2929 ss. Sulla discrezionalità legislativa nel determinare i criteri della competenza per territorio, cfr. Corte cost., 23 giugno 1994, sent. n. 280, ivi, 2475 ss., con nota di P. Ventura, *Nuove contestazioni e incompetenza per territorio*, ove la Corte ha ritenuto che il criterio del *forum commissi delicti* corrisponde non solo a finalità di economia processuale ma anche a rendere più agevole l'esercizio del diritto di difesa. In tale ottica, «deroghe a tale criterio, comportando una maggior gravosità delle modalità di esercizio del diritto di difesa, possano ritenersi legittime se sorrette da motivi di salvaguardia di interessi ritenuti, non irragionevolmente, degni di tutela».

[10] La Corte richiama espressamente Corte. cost., 23 aprile 1993, sent. n. 217, in *Giur. cost.*, 1993, 1622 ss.; Giur. cost., 3 giugno 1992, sent. n. 269, ivi, 1992, 2065 ss.

[11] Già M. Fumo, *La diffamazione mediatica*, Torino, 2012, 82; cfr. V. Pezzella, *La diffamazione*, Torino, II ed., 2016, 494.

pubblico ovvero la persona da loro delegata al controllo della trasmissione) o anche alla persona, citata a giudizio, che abbia concretamente commesso la diffamazione (come, ad esempio, il giornalista, l'autore televisivo o l'intervistato).

Della prima opinione una parte minoritaria della giurisprudenza[12], secondo cui, stante il divieto di applicazione analogica in materia, laddove il soggetto chiamato a rispondere del reato non possieda una delle qualifiche indicate espressamente all'art. 30, c. 1, l. 223 del 1990 debbano trovare applicazione le regole generali sulla competenza per territorio.

Prevalente, invece, il secondo indirizzo interpretativo che individua il foro competente, a prescindere da chi sia la persona imputata, nel luogo in cui risiede la persona offesa[13]. Secondo questa giurisprudenza, infatti, il dato testuale[14], fondato su una lettura congiunta dei commi 4 e 5, porta a ritenere differenziato a seconda della qualifica dell'autore il solo trattamento sanzionatorio e unificato, a prescindere da chi sia l'autore della diffamazione mediatica aggravata, il criterio di competenza territoriale[15].

A complicare ulteriormente la questione è intervenuta poi la recente dichiarazione di incostituzionalità dell'art. 30, c. 4, l. 223 del 1990[16] ad opera della sentenza n. 150

[12] A ben vedere, l'unica pronuncia che affronta in modo specifico il tema della competenza per territorio e che sposa tale interpretazione è Cass. pen., sez. I, 27 febbraio 1996, n. 1291, in *Ced Cass.*, n. 205281. Una serie di pronunce ulteriori, seppur spesso annoverate nell'indirizzo minoritario volto ad escludere l'estensione analogica della normativa ai soggetti diversi dai concessionari, in realtà si concentra prevalentemente sul tema della responsabilità penale per il reato di omesso controllo e del tutto marginalmente sulla competenza per territorio: Cass. pen., sez. II, 23 aprile 2008, n. 34717, ivi, n. 240687; cfr. Cass. pen., sez. V, 6 ottobre 2014, n. 50987, ivi, n. 261907; Cass. pen., sez. V, 19 aprile 2017, n. 27823, ivi, n. 270557.

[13] Cass. pen., sez. I, 13 dicembre 1994, n. 6018, in *Ced Cass.*, n. 200801; Cass. pen., sez. I, 13 dicembre 1996, n. 6793, ivi, n. 206755; Cass. pen., sez. I, 13 gennaio 2000, n. 269, ivi, n. 215382; Cass. pen., sez. V, 18 settembre 2014, n. 4158, ivi, n. 262168, escludendo a tal proposito che si verta in tema di interpretazione estensiva o analogica. In dottrina, favorevoli a questo indirizzo si veda, *inter alia*, G.M. Baccari, *La cognizione e la competenza del giudice*, Milano, 2011, 260; M. Fumo, *La diffamazione mediatica*, cit., 83 ss.

[14] In particolare, secondo tale esegesi l'inciso di cui al c. 4 dell'art. 30 l. 223 del 1990 «reati di diffamazione commessi attraverso strumenti consistenti nell'attribuzione di un fatto determinato» si riferisce a tutti i reati di diffamazione mediatica a prescindere dal soggetto agente mentre l'ulteriore espressione, sempre contenuta nel c. 4, «si applicano ai soggetti di cui al comma primo le sanzioni previste dall'art. 13 della legge 8 febbraio 1948, n. 47» riguarderebbe il solo trattamento sanzionatorio. In questo senso, il riferimento insito nel quinto comma ai reati del comma precedente determinerebbe la competenza per tutti i casi di diffamazione aggravata indipendentemente dall'autore.

[15] Si ritiene a tal proposito come tale indirizzo avrebbe il merito di «avere natura coerenziatrice di regimi di competenza territoriale, altrimenti divergenti se si ritenesse, viceversa, che i reati commessi dai soggetti nominati nel primo comma dell'art. 30 cit. dovessero seguire un foro differente da quello previsto come criterio generale dall'art. 9, comma 1, cod. proc. pen.». Così Cass. pen., sez. V, 15 marzo 2024, n. 26919, in *Ced Cass.*, n. 286578; analogamente Cass. pen., sez. V, 18 settembre 2014, n. 4158, cit., ove la Corte evidenzia come il diverso indirizzo interpretativo comporterebbe una irragionevole divergenza di competenze in quanto, per il medesimo fatto, l'autore immediato della diffamazione e chi è tenuto al controllo verrebbero sottoposti a giudizio innanzi a giudici diversi.

[16] L'incostituzionalità è stata affermata in via consequenziale rispetto alla declaratoria di illegittimità dell'art. 13 l. 8 febbraio 1948, n. 47: «Disposizioni sulla stampa», in *G.U.* 20 febbraio 1948, n. 43.

del 2021 della Corte costituzionale[17]. Ed è con questo ulteriore «dato inedito»[18] che il Giudice di legittimità si è trovato a confrontarsi, per la prima volta, con le pronunce in commento.

3. I rinvii pregiudiziali *ex* art. 24 *bis* c.p.p.

Il contrasto interpretativo appena delineato ha portato i giudici di merito ad azionare l'istituto introdotto dal d.lgs. 10 ottobre 2022, n. 150[19], e oggi disciplinato dall'art. 24 *bis* c.p.p.[20]. Da tre rinvii pregiudiziali[21] sono infatti scaturite le pronunce della Cassazione[22].

[17] Corte cost., 22 giugno 2021, n. 150, in *Giur. cost.*, 2021, 1563 ss., con commenti di G. Zampetti, *La "pronuncia doppia" nell'unico giudizio: i tempi della Corte e la discrezionalità del legislatore*; F. Medico, *Il* filo d'Arianna *dell'incostituzionalità prospettata e il parametro dimenticato (nota alla sent. n. 150 del 2021*); A. Tesauro, *«è la stampa, bellezza!»: la Corte costituzionale alle prese con la risposta carceraria alle lesioni mediatiche della reputazione* (ivi, 1835 ss.). Sulla pronuncia si veda inoltre, *inter alia*, C. Malavenda, *La sentenza n. 150/2021 della Corte Costituzionale in tema di diffamazione: i "pericoli per la democrazia" e il rischio che l'informazione, da "cane da guardia", si trasformi in "cucciolo da salotto"*, in *giurisprudenzapenale.com*, 21 luglio 2021.

[18] Così come evidenziato da Cass. pen., sez. V, 15 marzo 2024, n. 26919, cit.

[19] D.lgs. 10 ottobre 2022, n. 150: «Attuazione della legge 27.9.2021, 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», in *G.U.* 19 ottobre 2022, n. 245, Suppl. straord. n. 5.

[20] Sullo strumento di cui all'art. 24 *bis* c.p.p., rubricato «Rinvio pregiudiziale alla Corte di cassazione per la decisione sulla competenza per territorio», si veda, senza alcuna pretesa di completezza, G. Accatino, *Prime considerazioni intorno al nuovo art. 24-*bis *c.p.p.*, in *legislazionepenale.it*, 2023; R. Aprati, *L'intervento pregiudiziale della Corte di Cassazione sull'incompetenza territoriale*, in *Cass. pen.*, 2023, 1084 ss.; G. Casartelli, *Il rinvio pregiudiziale ex art. 24-bis c.p.p. per la decisione in ordine alla competenza territoriale introdotto dalla riforma Cartabia: note minime sui primi orientamenti della Corte di cassazione*, in *sistemapenale.it*, 25 settembre 2023; F. Cassibba, *sub art. 24-bis*, in A. Giarda-G. Spangher (a cura di), *Codice di procedura penale commentato*, I, VI ed., Milano, 2023, 676 ss.; A. Conti, *Il rinvio pregiudiziale in tema di competenza nell'interpretazione della Cassazione: efficientismo, discrezionalità e principio di legalità processuale*, in *Dir. pen. e proc.*, n. 12, 2023, 1620 ss.; R. Crepaldi, *L'udienza preliminare*, in V.A. Boga-R. Crepaldi-V. De Luca-L.N. Meazza-M. Moscardini-G. Stampanoni Bassi (a cura di), *Le indagini preliminari, l'udienza preliminare e la nuova udienza preliminare*, Torino, 2023, 245 ss.; E.N. La Rocca-A. Mangiaracina, *Le impugnazioni ordinarie: tra "efficienza" e snellimento*, in D. Castronuovo-M. Donini-E.M. Mancuso-G. Varraso (a cura di), *Riforma Cartabia. La nuova giustizia penale*, Padova, 2023, 921 ss.; R. Fonti, *Le nuove forme procedimentali del giudizio di legittimità e il rinvio pregiudiziale per la decisione sulla competenza per territorio*, in M. Bargis-H. Belluta (a cura di), *Commenti alla legge n. 134 del 2021 e ai decreti legislativi delegati - Vol. III - L'ennesima riforma delle impugnazioni fra aspettative deluse e profili controversi*, Torino, 2023, 194 ss.; M. Gialuz, *Per un processo penale più efficiente e giusto. Guida alla lettura della riforma Cartabia (profili processuali)*, in *sistemapenale.it*, 2 novembre 2022; S. Lonati, *Il rinvio pregiudiziale per la decisione sulla competenza per territorio: tra snodi interpretativi e prime applicazioni*, in L. Parlato (a cura di), *La nuova fisionomia delle impugnazioni*, Torino, 2024, 259 ss.; Id., *L'udienza preliminare*, in D. Castronuovo-M. Donini-E.M. Mancuso-G. Varraso (a cura di), *Riforma Cartabia,* cit., 706 ss.; C. Minella, *Difetto di competenza per territorio, "mano libera" della Suprema corte*, in A. Natalini (a cura di), *Riforma Cartabia: indagini preliminari e processo penale*, Gruppo24ore, Milano, 2023, 171 ss.; M. Oddis, *La cognizione "vincolata" della Suprema Corte in tema di rinvio pregiudiziale ex art. 24-bis c.p.p.*, in *sistemapenale.it*, 20 dicembre 2023; F.N. Ricotta, *I nuovi controlli sulla competenza per territorio*, in G. Spangher (a cura di), *La riforma Cartabia*, Pisa, 2022, 644 ss.; M. Pittiruti, *Un «rinvio pregiudiziale» per un processo penale efficiente. Luci e ombre dell'art. 24-bis c.p.p.*, in *sistemapenale.it*, 15 maggio 2023.

[21] Evidenzia la denominazione infelice dell'istituto S. Lonati, *Il rinvio pregiudiziale per la decisione sulla competenza per territorio: tra snodi interpretativi e prime applicazioni*, cit., 260; analogamente F.N. Ricotta, *I nuovi controlli sulla competenza per territorio*, cit., 644; M. Pittiruti, *Un «rinvio pregiudiziale» per un processo penale efficiente. Luci e ombre dell'art. 24-bis c.p.p.*, cit.

[22] Cass. pen., sez. V, 15 marzo 2024, n. 26919, in *Dir. e giust.*, 9 luglio 2024, con nota di C. Minnella,

Nell'ambito della prima ordinanza di rimessione[23], il Tribunale di Milano ha rilevato l'esistenza dei due diversi indirizzi giurisprudenziali e, pur propendendo per quello volto ad estendere il criterio del luogo di residenza della persona offesa a tutte le ipotesi di diffamazione mediatica aggravata, ha adito la Corte affinché decidesse sulla questione di competenza. Il Giudice di legittimità, ritenendo che il Tribunale avesse adeguatamente analizzato la questione e compiuto una preliminare valutazione di non manifesta infondatezza della stessa, «così da prospettare l'impossibilità di risolverla mediante l'utilizzo degli ordinari strumenti normativi»[24], ha dichiarato ammissibile il rinvio[25].
Del tutto analogamente, il Tribunale di Varese, nell'ambito della seconda ordinanza di rimessione[26], non solo ha dato atto dell'esistenza di due orientamenti giurisprudenziali tra loro contrapposti ma ha anche rigettato, di fatto, l'eccezione di incompetenza territoriale formulata *ex* art. 21 c.p.p. dalla difesa degli imputati[27]. La Corte, nel decidere per l'ammissibilità del rinvio, ha rilevato come l'unico giudice che ha titolo ad attivare lo strumento di cui all'art. 24 *bis* c.p.p. sia quello che «pur non ritenendosi incompetente, si rende conto che la diversa prospettazione operata dalle parti in punto di competenza territoriale non è manifestamente infondata, al punto che potrebbe successivamente originare una pronuncia attributiva di competenza territoriale ad un giudice diverso»[28]. La necessità di ricorrere al rinvio pregiudiziale solo in caso di «questioni di una certa

Diffamazione via TV: il forum commissi delicti è "sempre" quello della residenza della persona offesa; Cass. pen., sez. V, 14 giugno 2024, n. 34507, in *Ced Cass.*, n. 286958; Cass. pen., sez. V, 10 ottobre 2024, n. 41956, ivi, n. 287239.

[23] Da cui è originata Cass. pen., sez. V, 15 marzo 2024, n. 26919, cit.

[24] Cass. pen., sez. V, 15 marzo 2024, n. 26919, cit., richiamando espressamente Cass. pen., sez. I, 22 settembre 2023, n. 46466, in *Ced Cass.*, n. 285513.

[25] Alla Corte di cassazione spetta infatti il vaglio sull'ammissibilità del rinvio *ex* art. 24 *bis* c.p.p. alla luce del richiamo alle forme previste dall'art. 127 c.p.p., il cui c. 9 stabilisce la possibilità per il giudice di dichiarare con ordinanza l'inammissibilità dell'atto introduttivo del procedimento in camera di consiglio.

[26] Da cui è originata Cass. pen., sez. V, 14 giugno 2024, n. 34507, cit.

[27] Come noto, la richiesta di rinvio pregiudiziale deve essere presentata, ai sensi del c. 6 dell'art. 24 *bis* c.p.p., contestualmente alla formulazione dell'eccezione di incompetenza, pena la perdita della possibilità di riproporre la questione nel corso del procedimento. L'istanza costituisce quindi per la parte interessata un «onere», come evidenziato da R. Crepaldi, *L'udienza preliminare*, cit., 246. Per una critica nei confronti di tale previsione si veda, per tutti, S. Lonati, *Il rinvio pregiudiziale per la decisione sulla competenza per territorio: tra snodi interpretativi e prime applicazioni*, cit., 268, il quale evidenzia come sia «verosimile che tale rigido meccanismo preclusivo sarà capace di produrre, nella prassi, un unico effetto: "obbligare" la difesa a sollevare l'eccezione di incompetenza territoriale facendo seguire, sempre e comunque, la richiesta di rinvio pregiudiziale alla Cassazione. Questo per evitare, appunto, il rischio di vedersi precludere la possibilità di coltivare successivamente la questione una volta respinta».

[28] Cass. pen., sez. V, 14 giugno 2024, n. 34507, cit. Per il Giudice di legittimità è quindi escluso qualsiasi tipo di «delega» da parte del giudice di merito alla Cassazione – cosa che avverrebbe nel caso in cui il Tribunale compiesse il rinvio pur potendo giungere alla soluzione della questione con gli ordinari rimedi previsti dal codice o in assenza di una seria prospettazione alternativa in punto di competenza territoriale ad opera delle parti – essendo a tal proposito necessaria una preliminare delibazione di non manifesta infondatezza della questione. La Corte ha inoltre evidenziato come, laddove il giudice di merito si ritenga incompetente, questi abbia il dovere di trasmettere gli atti al pubblico ministero presso il giudice competente, salvo che quest'ultimo abbia già a sua volta trasmesso gli atti, in qual caso si dovrà sollevare conflitto ai sensi dell'art. 30 c.p.p. Al contrario, laddove il giudice di merito ritenga sussistente la propria competenza, questi potrà compiere il rinvio alla Corte di cassazione a patto che ritenga che la questione sollevata dalla parte sia, per quanto non condivisa, comunque fondata su «questioni di una certa serietà». Il tutto al fine di evitare «potenziali usi strumentali dell'istituto».

serietà» è stata ribadita dalla Corte anche nella decisione di ammissibilità del terzo rinvio pregiudiziale[29]. Nel caso di specie infatti, secondo la Cassazione, il contrasto giurisprudenziale in materia avrebbe in seguito potuto determinare una regressione del processo[30].

4. La scelta ermeneutica della Quinta Sezione

Una volta ritenuti ammissibili i rinvii pregiudiziali, la Corte di cassazione si è concentra-

[29] Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit. La Corte ha evidenziato come in assenza all'interno dell'art. 24 *bis* c.p.p. di espliciti parametri cui debba uniformarsi il giudice di merito nel disporre il rinvio pregiudiziale (al di là del fatto che tale rinvio debba avvenire tramite «ordinanza», necessariamente motivata ai sensi dell'art. 125, c. 3, c.p.p.) sia stata la stessa giurisprudenza di legittimità a tracciare il solco del nuovo istituto, inquadrando la «serietà» della questione come un suo «requisito implicito» (così Cass. pen., sez. IV, 25 ottobre 2023, n. 46181, in *Ced Cass.*, n. 285424) e affidando al giudice di merito il compito di «analizzare previamente le deduzioni prospettate dalle parti, […] tentare di comporle per raggiungere una decisione e […] illustrare compiutamente il percorso interpretativo in concreto effettuato, indicando le ragioni che non hanno consentito di risolvere la questione secondo gli ordinari strumenti processuali». Il tutto a pena di inammissibilità del rinvio stesso (cfr. Cass. pen., sez. III, 27 settembre 2023, n. 44932, ivi, n. 285334). Del resto, secondo la Corte a sostegno di tale «attività esplicativa» vi è la previsione di cui al c. 2 dell'art. 24 *bis* c.p.p., con la trasmissione da parte del giudice di merito alla Cassazione degli atti necessari alla risoluzione della questione. Sono inoltre da escludersi rinvii "esplorativi", essendo piuttosto necessaria una argomentata esposizione delle possibili soluzioni esegetiche alternative, oltre ad una completa descrizione dei fatti che permetta alla Corte una *plena cognitio* (Cass. pen., sez. IV, 25 ottobre 2023, n. 46181, cit.). Per alcuni rilievi critici nei confronti dell'inammissibilità per «a-specificità» o «mancanza di autosufficienza» dell'ordinanza di rimessione, S. Lonati, *Il rinvio pregiudiziale per la decisione sulla competenza per territorio: tra snodi interpretativi e prime applicazioni*, cit., 273 ss.; si veda, inoltre, E.N. La Rocca-A. Mangiaracina, *Le impugnazioni ordinarie: tra "efficienza" e snellimento*, cit., 923; F.N. Ricotta, *I nuovi controlli sulla competenza per territorio*, 647.

[30] Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit. La Corte ha ricordato a tal proposito come il nuovo istituto sia volto a prevenire la caducazione dell'attività processuale nel frattempo svolta in caso di una successiva dichiarazione di incompetenza. Evidente in tal senso, per la Cassazione, l'esigenza di dare attuazione non solo alle garanzie della precostituzione e naturalità del giudice ma anche dell'efficienza e della ragionevole durata del processo. Cfr. Cass. pen., sez. I, n. 20612, in *Ced Cass.*, n. 284720; Cass. pen., sez. V, 6 settembre 2023, n. 43638, ivi, n. 285306. Si veda, inoltre, Cass. pen., sez. V, 20 giugno 2023, n. 37783, in *DeJure*, ove, richiamando la relazione finale della Commissione Lattanzi (*Relazione finale e proposte di emendamenti al d.d.l. A.C. 2435*, in *giustizia.it*, 40) si è evidenziata l'opportunità «in ossequio ai principi costituzionali dell'efficienza e della ragionevole durata del processo, di "responsabilizzare il giudice di merito" nella valutazione del rinvio incidentale alla Corte regolatrice per la definizione della questione sulla competenza territoriale, orientando la scelta "solo al cospetto di questioni di una certa serietà", in modo da evitare potenziali usi strumentali dell'istituto derivanti da un automatismo defaticante connesso alla formulazione della eccezione. È, cioè, necessario che la decisione del giudice sia affidata ad un canone di ragionevole presunzione di fondatezza della questione». La logica efficientista e l'obiettivo di contrazione delle tempistiche processuali posti alla base dell'istituto sono evidenziati da A. Conti, *Il rinvio pregiudiziale in tema di competenza nell'interpretazione della Cassazione: efficientismo, discrezionalità e principio di legalità processuale*, cit., 1622; M. Gialuz, *Per un processo penale più efficiente e giusto. Guida alla lettura della riforma Cartabia (profili processuali)*, cit.; M. Pittiruti, *Un «rinvio pregiudiziale» per un processo penale efficiente. Luci e ombre dell'art. 24-bis c.p.p.*, cit. Del resto, le esigenze di celerità processuale erano presenti nella disciplina dell'(in)competenza per territorio già antecedentemente all'introduzione dell'art. 24 *bis* c.p.p., come evidenziato da G.M. Baccari, *La cognizione e la competenza del giudice*, cit., 397; cfr. M. Ricciarelli, *L'esercizio della funzione giurisdizionale: dalla competenza al riparto di attribuzioni*, cit., 120. Più in generale, sul rapporto tra le esigenze di economia e celerità e le regole di competenza territoriale in ambito penale si veda, per tutti, L.P. Comoglio, *Il principio di economia processuale*, vol. 2, Padova, 1980, 154 ss.

ta sulla risoluzione delle questioni di competenza territoriale poste alla sua attenzione[31]. Il «dato inedito» destinato ad «incidere significativamente sulle scelte interpretative»[32] è sicuramente la pronuncia n. 150 del 2021[33], con cui la Corte costituzionale ha dichiarato costituzionalmente illegittimo il c. 4 dell'art. 30 l. 223 del 1990 laddove prevedeva, «per i reati di diffamazione commessi attraverso trasmissioni consistenti nell'attribuzione di un fatto determinato» dai soggetti di cui al c. 1 della medesima disposizione[34], l'estensione della disciplina della diffamazione a mezzo stampa di cui all'art. 13 l. 8 febbraio 1948, n. 47, con l'applicazione della pena della reclusione da uno a sei anni cumulativamente ad una multa non inferiore a 258 euro[35]. La Quinta Sezione si è quindi interrogata sulla vigenza dello speciale criterio di determinazione della competenza di cui all'art. 30, c. 5, l. 223 del 1990 che, nel fissare nel «luogo di residenza della persona offesa» la competenza per territorio, espressamente richiama «i reati di cui al comma 4». Di qui il dilemma interpretativo.

Ebbene, secondo le pronunce in commento, la decisione del Giudice delle leggi ha avuto la funzione di elidere il trattamento sanzionatorio senza incidere sulla vigenza del criterio di competenza posto dall'art. 30, c. 5, l. 223 del 1990[36]. Per la Corte, infatti, è stata la stessa Consulta a chiarire la portata della propria decisione laddove ha evidenziato come, per effetto della dichiarazione di illegittimità, non si sia creato «alcun vuoto di tutela al diritto alla reputazione individuale contro le offese arrecate a mezzo della stampa, diritto che continua a essere protetto dal combinato disposto del secondo e del terzo comma dello stesso art. 595 cod. pen., il cui alveo applicativo si riespanderà in seguito alla presente pronuncia»[37]. Ne consegue la possibilità di ritenere il c. 5 dell'art.

---

31 Alla luce della comune soluzione interpretativa adottata dalla Quinta Sezione nelle tre pronunce in commento si procederà con una trattazione congiunta delle stesse evidenziando, laddove pertinente, le peculiarità di ciascuna di esse.

32 Cass. pen., sez. V, 15 marzo 2024, n. 26919, cit.

33 Corte cost., 22 giugno 2021, n. 150, cit.

34 Il concessionario privato, la concessionaria pubblica ovvero la persona da loro delegata al controllo della trasmissione.

35 La dichiarazione di illegittimità costituzionale dell'art. 30, c. 4, l. 223 del 1990 è avvenuta, in via consequenziale ai sensi dell'art. 27 l. 11 marzo 1953, n. 87, per effetto del riscontrato contrasto della disciplina di cui all'art. 13 l. 47 del 1948, con gli artt. 21 e 117, c. 1, Cost., in relazione all'art. 10 Cedu. Il menzionato art. 13 l. 47 del 1948, espressamente richiamato dal c. 4 dell'art. 30 l. 223 del 1990, applicava alla diffamazione commessa col mezzo della stampa, consistente nell'attribuzione di un fatto determinato, la pena della reclusione da uno a sei anni cumulativamente ad una multa non inferiore a 258 euro. L'indefettibilità dell'applicazione della pena detentiva, salvi i casi di giudizio di equivalenza o prevalenza di eventuali attenuanti, è stata così ritenuta incompatibile con il diritto di manifestazione del pensiero e, in particolare, con l'esigenza di non dissuadere, per effetto del timore della sanzione privativa della libertà personale, la generalità dei giornalisti dall'esercitare la propria funzione di controllo sull'operato dei pubblici poteri (come evidenziato da Cass. pen., sez. V, 15 marzo 2024, n. 26919, cit.). Sul trattamento sanzionatorio per il reato di diffamazione, antecedentemente all'intervento del Giudice costituzionale, si veda C. Melzi d'Eril, *La Corte Europea condanna l'Italia per sanzione e risarcimento eccessivi in un caso di diffamazione. Dalla sentenza qualche indicazione per la magistratura, il legislatore e le parti*, in *penalecontemporaneo.it*, 12 novembre 2013; C. Melzi d'Eril-G.E. Vigevani, *La riforma della diffamazione: da Strasburgo al Senato, passando per Palazzo della Consulta*, in questa *Rivista*, n. 3, 2020, 137.

36 Cass. pen., sez. V, 14 giugno 2024, n. 34507, cit.

37 Corte cost., 22 giugno 2021, n. 150, cit.

30 l. 223 del 1990 «tuttora vivente nel suo contenuto di competenza "speciale"»[38].
Risolta tale, prima questione interpretativa, la Cassazione si è quindi focalizzata sul contrasto giurisprudenziale relativo all'ambito di applicabilità della regola derogatoria di cui all'art. 30, c. 5, l. 223 del 1990. In tutte e tre le pronunce, la Quinta Sezione ha aderito a quell'indirizzo, già prevalente, che radica la competenza per territorio nel foro di residenza della persona offesa chiunque sia il soggetto chiamato a rispondere del reato[39].
A sostegno di tale tesi, la Suprema Corte ha innanzitutto richiamato il dato letterale dell'art. 30, c. 5, l. 223 del 1990, evidenziando come la disposizione in esame, nel richiamare i reati di cui al precedente c. 4, non faccia alcuna menzione dei soggetti nei cui confronti si procede[40]. Nessun richiamo testuale collega quindi il criterio del foro speciale alla categoria di soggetti indicati nel c. 1 dell'art. 30 l. 223 del 1990, neppure «per effetto della declaratoria di illegittimità costituzionale che ha eliminato dal mondo

[38] Cass. pen., sez. V, 15 marzo 2024, n. 26919, cit., secondo cui il c. 5 dell'art. 30 l. 223 del 1990 è da ritenersi richiamante non più il c. 4, ma l'art. 595 c.p. La Corte evidenzia, a tal proposito, come il comma quinto «si pone come norma dal contenuto di rinvio "mobile", quanto alle indicazioni riferite alla competenza territoriale, per i reati di diffamazione commessi tramite l'attribuzione di un fatto determinato ed a mezzo di strumenti radiofonici e televisivi – rinvio che la stessa declaratoria di incostituzionalità legittima, visto l'esplicito rimando della sentenza di incostituzionalità alla continuità punitiva tra art. 30, comma 4, l. n. 223 del 1990 e art. 595 cod. pen.». Pur ritenendo di dover pervenire alla medesima conclusione, offre un percorso argomentativo differente Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit., secondo cui, in realtà, l'art. 30, c. 5, l. 223 del 1990 compie un rinvio "statico" «con la conseguenza che non può dirsi mutato il contenuto dell'art. 30, comma 5, cit., sia pure a seguito della declaratoria di illegittimità costituzionale del precedente comma 4, il cui testo *in parte qua* è stato per l'appunto incorporato dal successivo comma 5, la cui portata precettiva […] non è incisa dal *dictum* della Consulta, come osservato relativo solo al trattamento sanzionatorio previsto per i delitti in discorso che continuano ad integrare, per l'appunto, fatti penalmente rilevanti *sub specie* della diffamazione […] senza incidere punto sul criterio di determinazione della competenza per territorio». Cfr. Cass. pen., sez. V, 14 giugno 2024, n. 34507, cit.: «[p]alesemente irragionevole risulterebbe ritenere che l'illegittimità del comma 4 voglia rendere impossibile applicare il comma 5, quanto al foro speciale, al caso della diffamazione aggravato dal fatto determinato e dal mezzo radiotelevisivo, sia che si ritenga la *ratio* dell'intervento della Corte costituzionale limitato al solo profilo sanzionatorio, sia che lo si ritenga radicalmente abrogativo del comma 4, nel quale caso si riespanderebbe *in toto* l'art. 595, comma 3, cod. pen.».

[39] I tre procedimenti *a quo* vedevano imputati soggetti non rientranti nelle categorie menzionate al c. 1 dell'art. 30 l. 223 del 1990 (il concessionario privato, la concessionaria pubblica ovvero la persona delegata al controllo della trasmissione radiofonica o televisiva). In particolare, con riferimento alla pronuncia n. 26919 del 2024, avanti al Tribunale di Milano erano imputati un autore e un conduttore della trasmissione televisiva "Le Iene", accusati di aver trasmesso un servizio televisivo sul c.d. delitto di Garlasco lesivo della reputazione di una donna di cui si insinuava il coinvolgimento nell'omicidio; ad un conduttore e ad un inviato del programma "Report" era invece contestato, nell'ambito del procedimento da cui è scaturita la pronuncia n. 34507 del 2024, di aver offeso la reputazione di un politico, all'epoca parlamentare e sottosegretario alla Presidenza del Consiglio dei Ministri, nonché della moglie e della cognata; infine, nel procedimento di cui alla pronuncia n. 41956 del 2024 erano imputati due autori di un servizio televisivo andato in onda nella trasmissione "Le Iene" nel corso del quale, secondo l'accusa, sarebbe stata lesa la reputazione di tre arbitri di calcio di serie A e B.

[40] Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit., ove la Corte evidenzia, a tal proposito, come sia il c. 4 dell'art. 30 l. 223 del 1990 a rinviare ai soggetti di cui al c. 1 dello stesso articolo «per estendere a questi ultimi le sanzioni previste dall'art. 13 l. n. 47 del 1948, da ultimo oggetto della declaratoria di illegittimità costituzionale». Inoltre, secondo la Corte, la seconda parte del c. 5 dell'art. 30 l. 223 del 1990 è da intendersi come «distinta ed indipendente da quella della prima parte dello stesso art. 30, comma 5 […] che invece rimanda anche ad altri commi che lo precedono (e, dunque, pure ad altre incriminazioni), ivi compreso il comma 1, e ad una disciplina (quella posta dall'art. 21 l. n. 47 del 1948) non inerente alla competenza per territorio».

giuridico il c. 4 dell'art. 30 nella parte sanzionatoria, l'unica effettivamente ed esplicitamente contenente il rimando ai "soggetti di cui al comma 1"»[41]. Ne deriva che, quando nel quinto comma dell'art. 30 l. 223 del 1990 si menzionano, ai fini della determinazione della competenza, i reati di cui al comma precedente, «questi comprendono anche la diffamazione consistente nell'attribuzione di un fatto determinato che sia stata commessa da persona non rientrante tra quelle indicate nel comma primo»[42].

Tale indirizzo, secondo la Cassazione, si pone in linea con quanto statuito dalla Corte costituzionale con la pronuncia n. 42 del 1996[43] e, in particolare, con l'obiettivo di attenuare lo squilibrio esistente tra chi commette la diffamazione mediatica aggravata e chi, del reato, subisce le conseguenze. Di qui, l'esigenza di incardinare il procedimento presso il giudice del luogo di residenza della persona offesa, più idoneo al giudizio in quanto presumibilmente più vicino al luogo di svolgimento dei fatti, e capace di assicurare una maggiore efficacia riparatoria, in caso di accertata sussistenza dell'azione diffamatoria, grazie «alla più ampia conoscenza che la stessa sentenza potrà ottenere nell'ambiente sociale normalmente frequentato dalla persona offesa»[44].

Dirimente poi, la maggiore «coerenza sistematica»[45] derivante dall'applicazione del criterio di residenza della persona offesa indipendentemente dalla qualifica del soggetto agente, nell'ottica di evitare l'«irragionevole divergenza di competenze» che deriverebbe dall'instaurazione, per un medesimo fatto di diffamazione, di più processi avanti a giudici diversi a seconda della persona chiamata a rispondere del reato[46].

Del resto, la Cassazione ha ricordato[47] come la ragionevolezza di un unico e stabile foro di competenza connesso al domicilio della persona offesa, ovvero il luogo dove si radicano i suoi interessi e le sue relazioni, trovi conferma nella giurisprudenza civile di legittimità e, in particolare, nell'ordinanza a Sezioni Unite n. 21661 del 2009[48]. Tale criterio, anche per il Giudice di legittimità civile, permette infatti di evitare una competenza "ambulatoria", potenzialmente lesiva del principio di precostituzione del giudice

[41] Cass. pen., sez. V, 15 marzo 2024, n. 26919, cit.

[42] Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit., che riporta testualmente quanto affermato da Cass. pen., sez. I, 13 gennaio 2000, n. 269, cit.

[43] Corte cost., 23 febbraio 1996, n. 42, cit., su cui *supra* § 1.

[44] Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit., richiamando testualmente Corte cost., 23 febbraio 1996, n. 42, cit.

[45] Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit.

[46] Cass. pen., sez. V, 14 giugno 2024, n. 34507, cit.: «la diversa interpretazione, conducente alla frammentazione della competenza territoriale, vedrebbe il foro speciale operare solo per i concessionari e non anche, ad esempio, per i giornalisti o gli intervistati, cosicché, per un medesimo fatto, chi è tenuto al controllo e l'autore immediato della diffamazione sarebbero chiamati a giudizio dinanzi a giudici diversi, il che integra una irragionevole divergenza di competenze».

[47] Cass. pen., sez. V, 15 marzo 2024, n. 26919, cit.; Cass. pen., sez. V, 14 giugno 2024, n. 34507, cit.; Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit.

[48] Cass. civ., sez. un., 13 ottobre 2009, ord. n. 21661, in *Ced Cass.*, n. 609467. Con questa pronuncia la Corte ha affermato il principio per cui, ai fini dell'individuazione del giudice territorialmente competente per un'azione di risarcimento del danno, il *forum commissi delicti* di cui all'art. 20 c.p.c. va individuato nel luogo del domicilio (o della sede della persona giuridica) o, in caso di diversità, anche della residenza del soggetto danneggiato, ovvero nel luogo in cui si realizzano le ricadute negative della lesione della reputazione.

di cui all'art. 25 Cost.[49], e di individuare il giudice competente in modo da favorire il danneggiato che, in controversie relative al risarcimento dei danni conseguenti al contenuto diffamatorio di una trasmissione televisiva, è solitamente il soggetto più debole[50]. Interessante notare a tal proposito come siano state le stesse Sezioni Unite civili a richiamare, a fondamento della propria interpretazione «in senso costituzionalmente orientato», proprio la sentenza n. 42 del 1996 della Corte costituzionale, affermando che «un'interpretazione dell'art. 20 cod. proc. civ., diversa da quella accolta, non essendo giustificata dalla diversa natura, civile o penale, dell'oggetto dei processi, potrebbe far sorgere seri di dubbi di legittimità costituzionale con riferimento all'art. 3 Cost.»[51].
Ad ulteriore suffragio della propria decisione, la Corte di cassazione ha infine richiamato il diritto dell'Unione europea che, proprio con riferimento ai casi di diffamazione, propende per l'adozione di un criterio di competenza che possa garantire gli obiettivi di prevedibilità, «assicurata dal principio del giudice naturale», e di buona amministrazione della giustizia, oltre che garantire un collegamento stretto tra l'autorità giurisdizionale e la controversia[52]. In questo senso, l'individuazione della competenza presso il giudice del luogo in cui la presunta vittima ha il proprio centro di interessi si pone, secondo le pronunce della Corte di giustizia richiamate dalla Cassazione, in conformità con tali obiettivi[53].
Alla luce di tali considerazioni, il Giudice di legittimità ha quindi affermato, con le pronunce in commento, che «in tema di diffamazione commessa attraverso trasmissioni radiotelevisive e consistente nell'attribuzione di un fatto determinato, anche successivamente alla sentenza n. 150 del 2021 della Corte costituzionale, la competenza territo-

[49] Cass. civ., sez. un., 13 ottobre 2009, ord. n. 21661, cit., ove le Sezioni Unite affermano che, ai sensi dell'art. 25 Cost., «i criteri di competenza [debbano essere] dettati dalla legge preventivamente e non in vista di singole controversie e abbiano natura generale e oggettiva. Conseguentemente, l'interpretazione dell'art. 20 c.p.c. deve portare al risultato di ancorare la competenza a un luogo certo e ben individuato, escludendo una competenza "ambulatoria"».

[50] Le Sezioni Unite hanno aderito, con tale pronuncia, ad una concezione del danno risarcibile inteso non come danno-evento, bensì come danno-conseguenza, attribuendo rilievo non alla mera potenzialità dannosa ma al pregiudizio effettivo e superando così quell'indirizzo che identificava il luogo ove era sorta l'obbligazione risarcitoria nel luogo di pubblicazione.

[51] Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit., richiamando testualmente Cass. civ., sez. un., 13 ottobre 2009, ord. n. 21661, cit.

[52] Cass. pen., sez. V, 14 giugno 2024, n. 34507, cit., richiamando le seguenti pronunce della Corte di giustizia: CGUE, C-451/18, *Tibor-Trans* (2019), ove la Corte era stata chiamata in sede di rinvio pregiudiziale a chiarire l'applicazione dell'art. 7, punto 2, del regolamento (UE) n. 1215/2012, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale; CGUE, C-800/19, *Mittelbayerischer Verlag KG/SI* (2021); CGUE, C-509/09 e C-161/10, *eDate Advertising e a.* (2011); CGUE, C-194/ 16, *Bolagsupplysningen e Ilsjan* (2017).

[53] Secondo Cass. pen., sez. V, 14 giugno 2024, n. 34507, cit., infatti, «la competenza del giudice del luogo in cui la presunta vittima ha il proprio centro degli interessi è conforme all'obiettivo della prevedibilità delle norme sulla competenza nei confronti del convenuto, poiché chi emette l'informazione lesiva, al momento della messa in rete della stessa (si trattava di una diffamazione a mezzo Internet), è in condizione di conoscere i centri degli interessi delle persone che ne formano oggetto, cosicché il criterio del centro degli interessi consente, al contempo, all'attore di individuare agevolmente il giudice al quale può rivolgersi e al convenuto di prevedere ragionevolmente dinanzi a quale giudice può essere citato». Non solo, secondo la Cassazione le «plurime competenze territoriali in ragione della diversa qualità degli autori del reato, come conseguenza dell'interpretazione qui non condivisa, vedrebbero leso il principio di buona amministrazione della giustizia, richiamato dalla CGUE».

riale deve essere stabilita applicando l'art. 30, comma 5, seconda parte, legge 6 agosto 1990, n. 223, con riferimento al luogo di residenza della persona offesa, chiunque sia il soggetto chiamato a rispondere della diffamazione, in forza della interpretazione costituzionalmente orientata conseguente alla sentenza n. 42 del 1996 della Corte costituzionale»[54].

5. La competenza per territorio in caso di concorso formale omogeneo di reati

Pur aderendo all'indirizzo esegetico appena delineato, nell'ambito della pronuncia n. 41956 del 2024 la Quinta Sezione, al fine di decidere sulla questione sollevata ai sensi dell'art. 24 *bis* c.p.p.[55], ha dovuto individuare altrimenti il giudice competente, non potendo operare nel caso di specie il criterio di cui all'art. 30, c. 5, l. 223 del 1990.
Nel giudizio *a quo*, infatti, erano imputati due soggetti accusati di aver commesso, con un'unica azione, tre delitti di diffamazione aggravata nei confronti di altrettante persone offese[56], reati ritenuti dalla Cassazione connessi ai sensi dell'art. 12, c. 1, lett. a) e b) c.p.p. Conseguentemente, secondo la Corte, non avrebbe dovuto trovare applicazione la regola derogatoria in materia di competenza per territorio prevista all'art. 30, c. 5, l. 223 del 1990, che «nulla dispone in relazione alla competenza per connessione», ma piuttosto il «criterio originario e autonomo di attribuzione della competenza»[57] di cui all'art. 16 c.p.p.[58].
Trattandosi di reati di pari gravità commessi con un'unica azione, la Suprema Corte ha però constatato l'impossibilità di determinare, nel caso di specie, la competenza ai sensi dell'art. 16 c.p.p., dovendosi quindi ricorrere, secondo l'insegnamento delle Sezioni Unite[59], ai criteri di cui agli artt. 8 e 9, c. 1, c.p.p., in grado di ancorare la competenza

[54] Così Cass. pen., sez. V, 14 giugno 2024, n. 34507, cit. Del tutto analogamente Cass. pen., sez. V, 15 marzo 2024, n. 26919, cit.; Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit.

[55] La Corte ha a tal proposito evidenziato come non sia vincolata, nella propria decisione sulla competenza, alle indicazioni del giudice di merito che ha trasmesso gli atti e, «fermo restando l'ancoraggio alla prospettazione fattuale introdotta dall'organo dell'accusa […] è chiamata a valutare, discrezionalmente e in piena autonomia, se la qualificazione giuridica del fatto storico (nelle sue componenti di condotta, evento e nesso causale) […] sia corretta, procedendo – in caso contrario – a delineare essa stessa l'esatta definizione da attribuirgli, con la conseguente designazione dell'organo giudiziario chiamato a giudicare sullo stesso», così Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit., richiamando testualmente Cass. pen., sez. I, 26 gennaio 2022, n. 5610, in *Ced Cass.*, n. 282724 (in materia di conflitti negativi di competenza).

[56] Come già evidenziato, il giudizio di merito vedeva imputati gli autori di un servizio televisivo andato in onda nella trasmissione "Le Iene", accusati di aver leso la reputazione di tre arbitri di calcio a cui era stata attribuita un'ipotesi di frode sportiva.

[57] Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit., citando testualmente Cass. pen., sez. un., 28 febbraio 2013, n. 27343, in *Ced Cass.*, n. 255345. In dottrina, sulla competenza per connessione come criterio originario e autonomo di attribuzione della competenza si veda, senza pretesa di completezza, G.M. Baccari, *La cognizione e la competenza del giudice*, cit., 269; F. Cordero, *Procedura penale*, cit., 147; O. Mazza, *I soggetti*, in Aa.Vv., *Procedura penale*, IX ed., 2024, Torino, 104; R. Casiraghi, *Competenza per connessione e giudice naturale*, in *Cass. pen.*, n. 12, 2013, 4492 ss.

[58] Ai sensi del quale, come noto, è competente il giudice per il reato più grave e, in caso di pari gravità, il giudice competente per il primo reato.

[59] Cass. pen., sez. un., 16 luglio 2009, n. 40537, in *Ced Cass.*, n. 244330.

a «un luogo ricollegabile *oggettivamente* all'illecito»[60]. Secondo il Giudice di legittimità, in questi casi è infatti necessario «assicurare, per quanto possibile, il collegamento tra competenza territoriale e luogo di manifestazione del reato, o almeno di un segmento del complesso criminoso, garantendo il principio, di valore costituzionale, della "fisiologica allocazione" del processo nel *locus commissi delicti*»[61].

Con specifico riferimento al delitto di diffamazione mediatica aggravata, poi, laddove sussista un concorso formale omogeno non solo non si potrà ricorrere all'art. 16 c.p.p. – in quanto reati di pari gravità commessi con un'unica azione – ma neppure all'art. 8 c.p.p.[62], in quanto espressamente derogato dal criterio speciale di cui all'art. 30, c. 5, l. 223 del 1990 che, a sua volta, non potrà trovare applicazione in caso di connessione *ex* art. 12, c. 1, lett. b). Piuttosto, ci si dovrà affidare alla regola di cui all'art. 9, c. 1, c.p.p., con l'individuazione della competenza presso il giudice dell'ultimo luogo in cui sia avvenuta una parte dell'azione o dell'omissione[63].

Secondo la Cassazione, in definitiva, nei casi, come quello di specie, in cui non trovi applicazione il criterio di favore per la persona offesa di cui all'art. 30, c. 5, l. 223 del 1990[64], occorrerà determinare la competenza attraverso un criterio, come quello di cui all'art. 9 c.p.p., che sia oggettivo, ancorato al fatto e alla sua presumibile capacità offensiva[65], senza possibilità di introdurre in via interpretativa criteri *extra legem*, come ad

[60] Secondo le Sezioni Unite solo qualora non sia possibile individuare il giudice competente ai sensi degli artt. 8 e 9, c. 1, c.p.p. troveranno applicazione i criteri suppletivi di cui ai c. 2 e 3 del medesimo art. 9 c.p.p. (presso il giudice della residenza, della dimora o del domicilio dell'imputato o, in subordine, presso il giudice del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato nel registro previsto dall'art. 335 c.p.p.).

[61] Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit., citando testualmente Cass. pen., sez. un., 16 luglio 2009, n. 40537, cit. Importante evidenziare come, secondo le Sezioni Unite, la regola di cui all'art. 9, c. 1, c.p.p. «risponde chiaramente alla *ratio* di affidare il giudizio ad un giudice che, per essere quello dell'ultimo luogo dove si è realizzata parte della condotta, risulta, probabilmente, il più vicino al contesto ambientale in cui si è perfezionato l'illecito».

[62] Secondo la Quinta Sezione, in ogni caso, anche a voler ritenere applicabile l'art. 8, c. 1, c.p.p. «nulla cambierebbe nella specie al fine della determinazione della competenza» in quanto, nel caso sottoposto al suo esame il luogo di consumazione del reato – ovvero il luogo in cui è avvenuta la percezione della trasmissione televisiva e del suo contenuto offensivo da parte di almeno due soggetti diversi dal soggetto agente e dalla persona offesa – non sarebbe individuabile e dovrebbe dunque farsi comunque applicazione dell'art. 9 co. 1 c.p.p.». Così Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit.

[63] Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit. La Corte ha evidenziato come rimanga «fermo il rapporto *logico* tra il medesimo art. 30, comma 5, cit. e l'art. 8 cod. proc. pen., nel senso che il primo costituisce norma speciale la cui operatività esclude l'applicazione del secondo. Ragion per cui, in tali ipotesi — tra le quali rientra ovviamente la presente — non si *rispande* la sfera di operatività delle regole generali poste dall'art. 8 cod. proc. pen. Il che non determina alcuna impossibilità di determinare la competenza, perché l'art. 30, comma 5, l. n. 223 del 1990 non deroga alle regole suppletive poste dall'art. 9 cod. proc. pen.».

[64] A tal proposito, la Corte sembra affermare che l'art. 30, c. 5, l. 223 del 1990 non troverebbe applicazione «nei casi in cui, come nel presente, sono diversi i luoghi di residenza degli offesi», così Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit. In realtà, proprio seguendo il ragionamento della Quinta Sezione, nei casi di connessione di cui all'art. 12, c. 1, lett. b) c.p.p. non potrà mai trovare applicazione, a prescindere dalla diversità o meno del luogo di residenza delle persone offese, tale criterio dovendo piuttosto applicarsi quello, del tutto autonomo, di cui all'art. 16 c.p.p. (facendo ricorso, semmai, al criterio di cui all'art. 9, c. 1, c.p.p.).

[65] Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit., richiama testualmente Cass. pen., sez. un., 16 luglio 2009, n. 40537, cit., secondo cui: «la radicazione della competenza nel luogo di manifestazione

esempio il luogo di residenza della prima persona offesa querelante[66].
Alla luce di tale percorso ermeneutico, la Cassazione ha quindi dichiarato, ai sensi dell'art. 24 *bis* c.p.p., l'incompetenza del Tribunale di Bologna, individuando il giudice competente nel Tribunale di Monza, nel cui circondario si trova la sede dell'emittente da cui è stato trasmesso il servizio televisivo, individuato come ultimo luogo in cui è avvenuta una parte dell'azione ai sensi dell'art. 9, c. 1, c.p.p., e ha disposto la trasmissione degli atti al Procuratore della Repubblica presso il medesimo Tribunale.

6. Rilievi conclusivi

Le pronunce in commento aderiscono a quel condivisibile indirizzo, già maggioritario in giurisprudenza, che estende la regola derogatoria di cui all'art. 30, c. 5, l. 223 del 1990 a tutti i reati di diffamazione aggravata, indipendentemente dalla qualifica del soggetto agente. È questa, infatti, l'interpretazione che emerge dalla *littera legis* e, in particolare, dalla lettura congiunta dei c. 4 e 5 della citata disposizione. Altrettanto condivisibile l'esegesi della Quinta Sezione relativa alle conseguenze della pronuncia di incostituzionalità dell'art. 30, c. 4, l. 223 del 1990, limitate al solo profilo sanzionatorio.
Detto questo, le premesse e lo sviluppo del percorso argomentativo seguito dalla Cassazione, che traggono linfa dalla pronuncia della Corte costituzionale n. 42 del 1996, si prestano tuttavia ad alcuni rilievi critici.
Il "peccato originale" della disciplina derogatoria di cui all'art. 30, c. 5, l. 223 del 1990 è quello di radicare la competenza per territorio del reato di diffamazione a mezzo radiotelevisivo, laddove aggravato dall'attribuzione di un fatto determinato, nel luogo di residenza della persona offesa. La *ratio* della previsione, ben delineata dalla Consulta nel 1996, è quella di un *favor* nei confronti dell'offeso dal reato, permettendo a quest'ultimo di attivarsi, a difesa della propria reputazione, più celermente e a costi ridotti, davanti ad un giudice ritenuto più idoneo al giudizio grazie «alla sua presumibile vicinanza con il luogo di svolgimento» dei fatti[67].
Quest'impostazione, sin dall'utilizzo della locuzione «foro competente» al c. 5 della

del reato esprime [...] un valore di rilevanza costituzionale […] è quindi evidente, già sulla sola base di questi principi generali e valori costituzionali, che in caso di dubbio debba essere preferita quella interpretazione che privilegi comunque la necessaria presenza di un collegamento della competenza territoriale con il luogo di commissione di almeno uno dei diversi reati commessi, anche quando tale luogo non sia accertato con riferimento al reato più grave, rispetto ad altre interpretazioni che possano portare ad una competenza territoriale del tutto sganciata dal luogo di manifestazione di almeno una parte della complessa fattispecie criminale».

[66] Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit., secondo cui: «la determinazione della competenza *ex* art. 30, comma 5, l. n. 223 del 1990, in ragione del foro del "primo querelante" […] non è previsto dalla legge, a prescindere dal fatto che i tre offesi abbiano sporto congiuntamente un'unica querela; e non possono neppure avere rilievo la circostanza […] che sarebbe stato […] il primo degli offesi ad avere contezza del fatto in contestazione e ad attivarsi […] perché si procedesse, e tantomeno l'adesione di questi ultimi alla determinazione della competenza *ratione loci* alla luce della residenza del […], elementi tutti estranei alle regole di determinazione della competenza […] oltre che incompatibili con i parametri – indipendenti dalla volontà dei soggetti processuali – cui deve essere affidata l'individuazione del giudice naturale precostituito per legge che deve conoscere la regiudicanda».

[67] Corte cost., 23 febbraio 1996, n. 42, cit.

disposizione[68], tradisce un approccio più consono al giudizio civile (e al rapporto tra attore e convenuto) rispetto al processo penale, fondato sulla struttura triadica, scolpita nell'art. 111, c. 2, Cost, per cui accusa e difesa sono poste, in condizioni di parità, dinanzi al giudice terzo e imparziale. In tale assetto, la competenza per territorio, determinata nel luogo in cui il reato è stato consumato ai sensi dell'art. 8, c. 1, c.p.p., esprime il tradizionale significato della garanzia del giudice naturale di cui all'art. 25 Cost., inteso come l'organo giurisdizionale radicato sul territorio in cui si è svolta l'azione criminosa[69]. Ecco quindi che, in ambito penale, tale garanzia porta con sé una duplice valenza: da un lato, è interesse dell'imputato non essere distolto dal giudice naturale; dall'altro, è interesse della collettività che il processo si celebri laddove sono maggiori il coinvolgimento sociale e l'attenzione per l'accertamento del reato e delle relative responsabilità[70].

Viceversa, la disciplina derogatoria in tema di diffamazione mediatica aggravata, nell'ottica di tutelare la persona offesa rispetto ai «poteri forti» dei *mass media*[71], impone all'imputato di privarsi del "suo" giudice naturale (dimenticandosi che, nel processo penale, l'unica figura meritevole di tutela rispetto al "potere forte" dello Stato è proprio il soggetto nei cui confronti è mossa l'accusa[72]) e individua la competenza presso un giudice, quello della residenza dell'offeso, che sarà il più vicino allo svolgimento dei fatti solo laddove essa venga a coincidere con il *locus commissi delicti*.

---

[68] Come già evidenziava autorevolmente T. Padovani, *Art. 30*, in E. Roppo-R. Zaccaria (a cura di), *Il sistema radiotelevisivo pubblico e privato*, Milano, 1991, 511.

[69] O. Mazza, *I soggetti*, cit., 100.

[70] *Ibid.* Cfr. G. Ubertis, *"Naturalità" del giudice e valori socioculturali nella giurisdizione*, in *Riv. it. dir. proc. pen.*, 1977, 1073 ss. Sulle diverse concezioni sviluppatesi in merito alla concezione di "giudice naturale", senza pretesa di completezza in una vasta letteratura, A. Bellocchi, *I requisiti di naturalità e precostituzione del giudice*, in G. Dean (a cura di), *Fisionomia costituzionale del processo penale*, Torino, 2007, 73 ss.; F. Caprioli, *Precostituzione, naturalità e imparzialità del giudice nella disciplina della rimessione dei processi*, in *Cass. pen.*, 2002, 2597 ss.; G. Conso, *Limiti inerenti al principio della certezza del giudice e rimessione del procedimento per legittimo sospetto o gravi motivi di ordine pubblico*, ivi, 1962, 241; A. Dalia, *Sulla precostituzione del giudice naturale come fondamentale garanzia di certezza per l'imputato, con particolare riguardo ai rapporti tra la competenza penale dei consoli e dei comandanti di porto*, in *Riv. it. dir. proc. pen.*, 1965, 516; A. Diddi, *La rimessione del processo penale*, Milano, 2000, 125 ss.; L. Giuliani, *Rimessione del processo e valori costituzionali*, Torino, 2002, 101; V. Grevi, *Davvero legittima la competenza del giudice non specializzato nei confronti del minore coimputato con maggiorenni?*, in *Giur. cost.*, 1966, 121 ss.; G. Ichino, *Precostituzione e naturalità del giudice nello spostamento di competenza per materia previsto dalla legge 14 ottobre 1974, n. 497 (Nuove norme contro la criminalità)*, in *Riv. it. dir. proc. pen.*, 1976, 578 ss.; M. Nobili, *Commento all'art. 25 comma 1 Cost.*, in G. Branca (diretto da), *Commentario della Costituzione*, Bologna-Roma, 1981, 189 ss.; M. Pisani, *La garanzia del «giudice naturale» nella Costituzionale italiana*, in *Riv. it. dir. proc. pen.*, 1961, 418 ss.; A. Pizzorusso, *Giudice naturale*, in *Enc. giur. Treccani*, XVI, Roma, 1989, 5; M. Ricciarelli, *L'esercizio della funzione giurisdizionale: dalla competenza al riparto di attribuzioni*, in G. Spangher (diretto da), *Trattato di procedura penale*, Torino, 2008, 44; G. Sabatini, *La competenza surrogatoria ed il principio del giudice naturale nel processo penale*, in *Riv. it. dir. proc. pen.*, 1962, 947; E. Somma, *«Naturalità» e «precostituzione» del giudice nell'evoluzione del concetto di legge*, ivi, 1963, 826 ss.; G. Spangher, *La rimessione dei procedimenti. - Vol. I - Precedenti storici e profili di legittimità costituzionale*, Milano, 1984, 286; C. Taormina, *Giudice naturale e processo penale*, Roma, 1972. Si veda inoltre, anche per ulteriori riferimenti bibliografici, G.M. Baccari, *La cognizione e la competenza del giudice*, cit., 123 ss.

[71] Come evidenziato da Cass. pen., sez. V, 15 marzo 2024, n. 26919, cit.

[72] Evidente, a tal proposito, l'intenzione di anticipare, in un momento precedente l'accertamento processuale del reato la tutela della persona offesa, preparando il terreno a quella maggior tutela riparatoria che deriverà, in caso di pronuncia di condanna, dall'emissione della sentenza da parte del giudice del luogo di residenza della persona offesa. Cfr. Corte cost., 23 febbraio 1996, n. 42, cit.

Non è un caso, quindi, che il Giudice di legittimità con le pronunce in commento, nell'interpretare l'art. 30 l. 223 del 1990, abbia tratto spunto dalla giurisprudenza della Corte di giustizia, avente ad oggetto l'interpretazione di una previsione sulla competenza in ambito civile e commerciale, e dalle Sezioni Unite civili, chiamate a dirimere un contrasto interpretativo relativo all'individuazione del giudice competente per un'azione di risarcimento del danno. Proprio le Sezioni Unite civili, del resto, hanno a loro volta richiamato, a fondamento della propria decisione, la pronuncia n. 42 del 1996 della Corte costituzionale, sul presupposto che un differente esito interpretativo, rispetto al domicilio della persona offesa, non potesse essere «giustificat[o] dalla diversa natura, civile o penale, dell'oggetto dei processi»[73].

Eppure, le peculiarità del processo penale e dei valori in esso coinvolti, rispetto al giudizio civile, sono state evidenziate dalla stessa Corte costituzionale in altra occasione, rimarcando come il principio del "giudice naturale" di cui all'art. 25 Cost. assuma in ambito penale «un carattere del tutto particolare, in ragione della "fisiologica" allocazione di quel processo nel *locus commissi deliciti* […] giacché la celebrazione di quel processo in "quel" luogo, risponde ad esigenze di indubbio rilievo, fra le quali, non ultima, va annoverata anche quella – più che tradizionale – per la quale il diritto e la giustizia devono riaffermarsi proprio nel luogo in cui sono stati violati»[74]. Ciò non significa, ovviamente, che l'imputato non possa «ragionevolmente» subire lo spostamento del processo dal "suo" giudice naturale ma ciò dovrà avvenire solo a fronte di «interessi superiori»[75], tra i quali non può essere di certo ricompresa la (pur legittima) tutela della persona offesa dal reato[76].

È del tutto evidente, in definitiva, come la disciplina derogatoria di cui all'art. 30, c. 5, l. 223 del 1990 sconti le difficoltà del legislatore nell'individuazione del *locus commissi delicti* del reato di diffamazione a mezzo radiotelevisivo[77] e adotti, come soluzione, il criterio della residenza della persona offesa[78]. Eppure, proprio una delle pronunce in commen-

[73] Cass. civ., sez. un., 13 ottobre 2009, ord. n. 21661, cit.

[74] Corte cost., 5 aprile 2006, n. 168, in *Giur cost.*, 2006, 1489 ss.

[75] Cfr. F. Cordero, *Procedura penale*, cit., 109 ss., ove l'Autore evidenzia, con riferimento al giudice naturale quale «giudice individuato secondo criteri che includano riferimenti al locus delicti», che sussiste «un interesse costituzionalmente tutelato al processo in quella tal sede, davanti al "suo" pubblico, ma cede a interessi superiori: ad esempio, quando l'ambiente turbato imponga una rimessione (art. 45)».

[76] Si veda, a tal proposito, Corte cost., 5 aprile 2006, n. 168, cit., ove la Corte, a fronte di una questione di legittimità costituzionale dell'art. 45, c. 1, c.p.p. con riferimento agli artt. 3, 24, c. 2, 11, c. 2, Cost., ha evidenziato come «perché l'imputato possa ragionevolmente subire lo spostamento del processo dal suo "giudice naturale", deve essere il "suo" processo (vale a dire quello penale) ad essere turbato da gravi situazioni locali. Quindi, solo i protagonisti necessari sono logicamente abilitati ad attivare il relativo ed eccezionale meccanismo di scrutinio, e non altri, che possono assumere soltanto la veste di cointeressati o controinteressati rispetto alle posizioni assunte dall'imputato e dal pubblico ministero».

[77] G. Corrias Lucente, *Prime osservazioni sugli aspetti penali della legge di disciplina del sistema radiotelevisivo*, cit., 432.

[78] T. Padovani, *Art. 30*, cit., 511 ss. A proposito della soluzione prescelta G. Corrias Lucente, *Prime osservazioni sugli aspetti penali della legge di disciplina del sistema radiotelevisivo*, cit., 433, evidenzia come tale criterio desti perplessità laddove la residenza «sia un dato meramente formale ed altrove (nel reale domicilio) si risentano in misura più estesa gli effetti della diffamazione. Ed altrettanto illegittima appare la determinazione speciale della competenza per altri due casi: che l'offesa venga trasmessa da un'emittente regionale e che l'offeso risieda fuori dal territorio in cui si riceve la trasmissione, o che l'offeso risieda all'estero; in questo caso non si vede come possa applicarsi il criterio speciale […] Non

to dimostra come, in realtà, vi sia una valida alternativa[79], conforme al principio del giudice naturale di cui all'art. 25, c. 1, Cost., nella regola suppletiva di cui all'art. 9, c. 1, c.p.p., che consente di stabilire la competenza nell'«ultimo luogo in cui è avvenuta una parte dell'azione o dell'omissione», cioè il luogo in cui la trasmissione televisiva è andata in onda. In questo modo, verrebbe assicurata una maggiore coerenza sistematica attraverso un raccordo con l'ipotesi di diffamazione mediatica non aggravata, in relazione alla quale, stante l'inevitabile concorrenza di più giudici competenti derivante dalla cognizione dell'informazione offensiva (momento consumativo del reato) da parte di più persone, trovano nei fatti applicazione proprio le regole suppletive di cui all'art. 9 c.p.p.[80].

Opzione alternativa, quella qui proposta, che, stante la *littera legis* dell'art. 30, c. 5, l. 223 del 1990, non potrebbe essere frutto di interpretazione giurisprudenziale ma dovrebbe essere adottata per via legislativa o per effetto di una declaratoria di incostituzionalità della disposizione derogatoria ad opera della Consulta, attraverso la valorizzazione del principio del giudice naturale di cui all'art. 25 Cost.[81]. In quest'ultima ipotesi, anche per la diffamazione a mezzo radiotelevisivo aggravata dall'attribuzione di un fatto determinato e a prescindere dall'esistenza di un concorso formale di reati, troverebbero applicazione la regola ordinaria sulla competenza di cui all'art. 8 c.p.p. e, in subordine, le regole suppletive di cui all'art. 9 c.p.p.

sembra in tali ipotesi (tutt'altro che eccezionali) rispettato il principio del giudice naturale».

[79] Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit. Come visto (*supra*, § 5) la Cassazione ha dovuto far ricorso a tale criterio a causa della sussistenza di un concorso omogeneo di reati nei confronti di una pluralità di persone offese. Sul punto, già F. Cordero, *Codice di procedura penale commentato*, Torino, 1989, 20, evidenziava l'*empasse* che avrebbe potuto crearsi quando siano contemporaneamente diffamate più persone residenti in luoghi diversi.

[80] Cfr. Cass. pen., sez. V, 21 aprile 2016, n. 33287, in *Ced Cass.*, n. 267703, che richiama, con riferimento alla diffamazione "telematica" Cass. pen., sez. V, 21 giugno 2006, n. 25875, ivi, n. 234528. Sul punto si veda anche Cass. pen., sez. V, 10 ottobre 2024, n. 41956, cit.

[81] O. Mazza, *I soggetti*, cit., 91, evidenzia che la Corte costituzionale, nel privare il requisito della "naturalità" di cui all'art. 25 Cost. di un'autonoma considerazione rispetto alla precostituzione, compie un vero e proprio «suicidio interpretativo non conforme ai princìpi dell'ermeneutica, in particolare quella costituzionale, e soprattutto foriero di un'ingiustificata riduzione delle garanzie processuali». Cfr. F. Cordero, *Relazione su «Connessione di procedimenti e giudice naturale»*, in Aa.Vv., *Connessione di procedimenti e conflitti di competenza. Atti del X convegno di studio "E. De Nicola"*, Milano, 1976, 54.

Gli insulti sessisti sono una forma di violenza sulle donne. E come tali vanno puniti anche se realizzati mediante i social

Jacopo Antonelli Dudan

Tribunale di Torino, sez. Giudici per le Indagini Preliminari, ord. 17 gennaio 2025

Keywords

diffamazione – sessismo – reputazione – social network – violenza di genere

Qualche settimana fa aveva destato stupore – quanto meno in chi scrive – la notizia che un PM di Torino avesse formulato richiesta di archiviazione in un caso di diffamazione on-line, in cui la querelante lamentava l'offesa alla propria reputazione posta in essere da una serie di utenti social che, con riguardo a un presunto tradimento dalla stessa posto in essere nei confronti dell'ex fidanzato e da questi diffuso con un video registrato in occasione di una festa di compleanno, si erano espressi con epiteti a dir poco volgari e offensivi, tra cui – a mero titolo di esempio – zoccola, troia, mignotta, bocchinara, puttana, vacca e così via, ricorrendo al peggior campionario di insulti offerti dalla lingua italiana.

Nel motivare la propria richiesta, il PM, oltre a ritenere non identificabili gli autori delle offese, normalmente celati dietro pseudonimi o false generalità, aveva sostanzialmente ritenuto che quei post fossero espressione del diritto di critica, rispettosi dei tradizionali criteri individuati dalla costante giurisprudenza: l'interesse pubblico, derivante dalla (presunta) notorietà della persona offesa e dell'ex fidanzato; la verità del fatto (o meglio, del presupposto fattuale della critica), perché il tradimento sarebbe stato dichiarato dall'ex fidanzato e non smentito dall'interessata; la continenza espressiva, perché il "luogo" della manifestazione del pensiero – il noto social Facebook, caratterizzato dal costante o quanto meno frequente uso di un linguaggio "sopra le righe" – avrebbe determinato una generalizzata desensibilizzazione e legittimato l'uso di non misurati e ineleganti.

È di questi giorni la decisione del GIP di Torino, che, non accogliendo la richiesta di archiviazione e disponendo che il PM debba svolgere indagini di natura tecnica per individuare concretamente i responsabili degli insulti via social, compie un interessante *excursus* sui rapporti tra la diffamazione commessa tramite tecnologie dell'informazio-

ne e della comunicazione (le cosiddette TIC) e la violenza sulle donne.
Ad avviso del GIP, nella vicenda sottoposta alla sua attenzione va per prima cosa stabilito se si versi in un'ipotesi di esercizio del diritto di critica: per compiere tale valutazione, il giudice ritiene che debbano essere considerati non solo i "canonici" limiti per la sussistenza della scriminante in parola (così come elaborati dalla costante giurisprudenza in materia), ma anche le caratteristiche dei commenti stessi.
Nel caso di specie, infatti, questi ultimi risultano così strettamente collegati alla morale sessuale femminile e a tal punto rivolti in modo esclusivo al genere femminile da poter essere qualificati come "comportamenti sessisti" e "discorsi d'odio" – realizzati, per l'appunto, con l'utilizzo delle tecnologie dell'informazione e della comunicazione (c.d. TIC) – e, in ultima analisi, vere e proprie manifestazioni di violenza sulle donne, così come codificata dalla più recente normativa comunitaria.
A sostegno di tale affermazione, il giudice ricorda *in primis* come una fondamentale definizione della violenza contro le donne sia fornita dalla Convenzione di Istanbul (firmata dal Comitato dei Ministri del Consiglio d'Europa nel 2011 e ratificata in Italia nel 2013), secondo cui deve considerarsi tale qualsiasi atto di violenza di genere perpetrata nei confronti di donne o che comunque colpisce le donne «in modo sproporzionato, che provochi o possa provocare danni o sofferenza fisica, sessuale, psicologica o economica, incluse le minacce di compiere tali atti».
In maniera analoga, la direttiva (UE) 2024/1385 del 14 maggio 2024 prende in considerazione tutte quelle ipotesi in cui «la violenza sia intrinsecamente connesso all'uso delle tecnologie dell'informazione e della comunicazione», facendo in tal modo riferimento non solo all'utilizzo di strumenti informatici per commettere una violenza in danno delle donne (si pensi alla diffusione illecita di materiale intimo, il c.d. *revenge porn*, o allo stalking on-line), ma anche ai discorsi d'odio sessista, vale a dire a tutte quelle situazioni in cui l'utilizzo dei social e in generale dei mezzi di comunicazione informatici (i c.d. TIC) determina una rapida e facile amplificazione dei commenti offensivi, accrescendo enormemente il rischio di provocare danni anche profondi in capo alla vittima o di aggravarne gli effetti, per effetto della possibile riproposizione temporale delle offese e della difficoltà – anche tecnica – a eliminarle per sempre una volta che si sono diffuse tramite il web.
Da ultimo, il GIP richiama la Raccomandazione del Consiglio d'Europa del 27 marzo 2019, che ha esplicitato il collegamento tra sessismo e violenza sulle donne affermando espressamente come esista «un continuum tra gli stereotipi di genere, le disparità di genere, il sessismo e la violenza contro le donne» e sottolineando come anche semplici atti di sessismo ordinario – come «commenti e battute sessiste apparentemente insignificanti e prive di conseguenze» – possano ben costituire forme di violenza contro le donne, perché si tratta di atti «spesso umilianti» che «contribuiscono a creare un clima sociale in cui le donne sono svilite, la loro autostima è ridotta e le loro attività e scelte vengono limitate, nel contesto lavorativo, nella sfera privata, in quelle pubblica e in rete».
Così delineato il perimetro normativo della definizione di violenza contro le donne, la conclusione del giudice appare sostanzialmente inevitabile e indiscutibile: i commenti degli utenti di Facebook nella vicenda in oggetto appaiono volti a stigmatizzare la

parte lesa unicamente in quanto donna e, come tali, risultano palesemente discriminatori ed espressione di odio e di violenza. Lungi dall'essere espressione di un giudizio critico, si tratta di commenti basati su stereotipi di genere, animati da una finalità esclusivamente offensiva così evidente da porli *ictu oculi* fuori da qualsiasi – pur ampio – perimetro del legittimo esercizio del diritto di critica.

Non di meno, con apprezzabile completezza argomentativa, il giudice ritiene doveroso procedere a un'analisi della vicenda anche secondo i noti presupposti del diritto di critica, vale a dire verità del fatto, interesse pubblico e continenza espressiva. Pur ponendosi nel solco della costante e maggioritaria giurisprudenza, la decisone in commento appare anche sotto questo profilo interessante, per la chiarezza con cui il Gip ribadisce i confini di quei requisiti, anche quando il luogo della contestata diffamazione non sia un salotto bene ma un social come Facebook, vale a dire un luogo dove chiunque può accedere e dire la sua.

Per quanto concerne la verità del fatto, viene ribadito come la critica, per quanto contenga necessariamente l'espressione di un giudizio di valore, debba necessariamente muovere da un presupposto di fatto, che deve essere vero e verificabile; qualora, dunque, il nucleo fattuale risulti insufficiente (perché non vero e non controllabile), il conseguente giudizio risulta gratuito e ingiustificato e, laddove offensivo, diffamatorio e perciò illecito. Applicando tale principio al caso di specie, risulta evidente come gli ignoti offensori non si premurino nemmeno di individuare e indicare quale sia il presupposto fattuale del proprio giudizio critico (ove mai possa ritenersi tale e non meramente espressivo di violenza, come già detto).

Del tutto inaccettabile risulta, peraltro, anche l'interpretazione proposta dal PM nella propria richiesta di archiviazione, secondo cui il nucleo fattuale risulterebbe vero nella misura in cui dovrebbe ritenersi vero quanto raccontato dall'ex fidanzato nel video (mai formalmente smentito dalla querelante), non foss'altro perché i commenti "incriminati" risultano totalmente distanti dall'evento concreto e da esso sganciati, sì che il presunto tradimento posto in essere dalla querelante risulterebbe non già il fatto su cui si sviluppa la critica degli utenti di Facebook, ma un mero pretesto utilizzato dai predetti per procedere a immotivati e inaccettabili insulti. In altri e più chiari termini, la critica presuppone pur sempre un ragionamento logico che, muovendo da un presupposto fattuale, conduca all'espressione di un giudizio: se quel presupposto manca o, comunque, non viene nemmeno indicato e il presunto giudizio si riduce a un immotivato insulto, si sta diffamando e non esercitando il diritto di critica. Che è esattamente quanto accaduto nel caso di specie.

Passando poi ad analizzare il criterio dell'interesse pubblico, correttamente il giudice lo considera del tutto mancante nella vicenda sottoposta al suo giudizio, posto che, a prescindere dalla notorietà (vera o presunta, maggiore o minore) del soggetto cui la notizia è riferita, il giudizio deve riguardare la dimensione pubblica della persona criticata; se, al contrario, il giudizio si riferisce esclusivamente alla sfera privata, esso si risolve in un attacco personale, come tale ingiustificato e inammissibile.

Da ultimo, il Gip si sofferma sul tema della continenza per ribadire che, pur se, in termini generali, l'esercizio del diritto di critica deve potersi esprimere anche con toni aspri e pungenti, talora persino inurbani, gli stessi non possono però trasformarsi in

invettive sproporzionate o, peggio, in espressioni gravemente infamanti. Anche tenendo conto, doverosamente, del luogo ove il commento viene espresso – Facebook nel caso *de quo* – e del differente contesto sociale cui tale luogo necessariamente rimanda, le parole utilizzate dagli autori dei post "incriminati" appaiono totalmente e «oggettivamente sopra le righe ed inutilmente umilianti», sì da qualificarsi come «veri e propri insulti», che mai e in nessun luogo possono ritenersi ammissibili e men che meno leciti. In conclusione, la decisione in commento, oltre a ricordare che – almeno per ora – l'insulto libero non è consentito nemmeno sui social più "popolari", ribadisce la punibilità di tutte quelle condotte verbali che si risolvono in offese sessiste e discriminazioni di genere, al di fuori di qualsiasi serio e argomentato giudizio.

Cronache

Documento di intesa in materia di informazione giudiziaria

tra Tribunale Ordinario di Milano, Procura della Repubblica presso il Tribunale di Milano, Ordine dei Giornalisti di Milano, Ordine degli Avvocati di Milano e Camera Penale di Milano

1. Premessa sulla genesi e sulle finalità del tavolo di confronto

Lo scorso 16 maggio 2023, il Presidente del Tribunale di Milano proponeva di avviare un tavolo di confronto, istituito e proseguito con i contributi della Procura della Repubblica presso il Tribunale di Milano, dell'Ordine dei Giornalisti di Milano, dell'Ordine degli Avvocati di Milano, della Camera Penale di Milano, "in tema di buone pratiche per le comunicazioni giudiziarie".

L'intento dichiarato e condiviso dal gruppo di lavoro è stato quello di "coniugare la presunzione di innocenza e una corretta e completa informazione", attraverso l'elaborazione di principi comuni e regole operative, rispettose del D.Lgs. 188/2021 e della normativa processuale. Resta invece estraneo alle considerazioni che seguono l'ambito della diffusione illecita di atti coperti da segreto o per i quali sussista un divieto di pubblicazione (v. artt. 114 e 329 c.p.p.); in entrambi i casi, si concorda che le condotte in violazione delle norme penali (artt. 326 e 684 c.p.), fatte salve le eventuali responsabilità disciplinari, dovranno essere perseguite con assoluta fermezza e attivazione investigativa, nell'interesse delle persone coinvolte, del procedimento penale e del sistema dell'informazione tutto.

Il gruppo di lavoro si impegna a proseguire nell'interlocuzione e nel monitoraggio dei comunicati emessi dalle Autorità Giudiziarie in intestazione, nonché delle conferenze stampa, anche al fine di verificare e migliorare il testo sottoscritto; saranno a questo fine tenute riunioni semestrali, su iniziativa di uno dei sottoscrittori.

Ferme restando le norme vigenti e la loro interpretazione, così come la rispettiva normativa deontologica che tutti gli attori del Tavolo richiamano come essenziale per un migliore funzionamento del sistema, si ritiene di poter condividere i principi che seguono, che saranno oggetto di diffusione anche culturale da parte di tutti gli aderenti, ad ogni soggetto terzo coinvolto (forze di polizia, personale amministrativo e cittadini).

2. La nozione di interesse pubblico ai sensi del D. Lgs. 188/2021

Recependo la Direttiva europea 343/16 in tema di rafforzamento della presunzione di innocenza, il d.lgs. 188/2021 è intervenuto sulle modalità di comunicazione da parte della Procura sui procedimenti penali, modificando l'art. 5 del d.lgs. 106/2006 in materia di rapporti con gli organi di informazione.

Il co. 2-bis dell'art. 5, così come modificato dal decreto citato, stabilisce che "la diffusione di informazioni sui procedimenti penali è consentita solo quando è strettamente necessaria per la prosecuzione delle indagini o ricorrono altre specifiche ragioni di interesse pubblico".

Sin dalla sua introduzione, le maggiori criticità si sono riscontrate proprio nella interpretazione del concetto di "interesse pubblico".

La genericità della locuzione si presta infatti a diverse e contrapposte interpretazioni, con il rischio di vanificare la finalità della norma. Si è pertanto avvertita l'esigenza, da parte di tutti i soggetti partecipanti al gruppo di lavoro, di giungere ad una definizione condivisa di "interesse pubblico" ai sensi del d.lgs. 188/2021, che muova dalla ratio della normativa e della Direttiva europea di cui è attuazione.

A tal fine si è tenuto conto, in particolare, delle seguenti disposizioni della Direttiva 343/2016:

- articolo 4, paragrafo 3, ai sensi del quale l'obbligo di non presentare gli indagati o imputati come colpevoli "non impedisce alle autorità pubbliche di divulgare informazioni sui procedimenti penali, qualora ciò sia strettamente necessario per motivi connessi all'indagine penale o per l'interesse pubblico".
- considerando 18 che chiarisce che "l'obbligo di non presentare gli indagati o imputati come colpevoli non dovrebbe impedire alle autorità pubbliche di divulgare informazioni sui procedimenti penali, qualora ciò sia strettamente necessario: per **motivi connessi all'indagine penale**, come nel caso in cui venga diffuso materiale video e si inviti il pubblico a collaborare nell'individuazione del presunto autore del reato, o per l'interesse pubblico, come nel caso in cui, **per motivi di sicurezza**, agli abitanti di una zona interessata da un presunto reato ambientale siano fornite informazioni o la pubblica accusa o un'altra autorità competente fornisca informazioni oggettive sullo stato del procedimento penale **al fine di prevenire turbative dell'ordine pubblico**. Il ricorso a tali ragioni dovrebbe essere limitato a situazioni in cui ciò sia ragionevole e proporzionato, tenendo conto di tutti gli interessi. In ogni caso, le modalità e il contesto di divulgazione delle informazioni non dovrebbero dare l'impressione della colpevolezza dell'interessato prima che questa sia stata legalmente provata".
- considerando 19 che fa "salvo il diritto nazionale a tutela della libertà di stampa e dei media".
- Muovendo dalle disposizioni sopra citate della direttiva 343/2016 sulla presunzione di innocenza e dai principi che disciplinano da una parte i rapporti tra Procura e stampa (più in generale i *media*) e dall'altra la piena esplicazione del diritto di informazione, si è convenuto che:

- la nozione di interesse pubblico di cui al D.lgs. 188/21 è un parametro specifico per l'Autorità Pubblica che presiede alla divulgazione delle informazioni sui procedimenti penali;
- esso non coincide con l'interesse pubblico che legittima i giornalisti a diffondere notizie e non può, quindi, essere interpretato alla luce di canoni della rilevanza della notizia previsti dalla giurisprudenza per l'esercizio del diritto di cronaca;
- la scelta del Legislatore comunitario di escludere dal campo di applicazione della Direttiva i giornalisti conferma la volontà di mantenere separati i due ambiti, proprio in ragione della diversità di ruolo e di funzioni tra giornalisti e autorità pubbliche.
- mentre l'esercizio del diritto di cronaca deve essere il più ampio possibile in ossequio all'art. 21 Cost. e può rispondere a criteri di rilevanza pubblica generale (pur nel rispetto di altri diritti fondamentali di pari rango, vedi infra), la facoltà del Procuratore di divulgare informazioni sui procedimenti penali è legata, invece, unicamente alle esigenze del procedimento penale.

Alla luce di quanto sopra, si conviene che:

a) l'**interesse pubblico** che consente al Procuratore della Repubblica di divulgare informazioni sui procedimenti penali (o di autorizzare la Polizia Giudiziaria a fornire informazioni tramite comunicati stampa) è connesso **alle esigenze del procedimento penale o alla particolare gravità del fatto reato.**
b) senza pretesa di tassatività, stante la specificità di ogni singolo caso e l'autonomia di valutazione del Procuratore nella valutazione del caso concreto, sussiste "interesse pubblico", vale a dire:
    - la sussistenza di motivi connessi all'indagine penale (ad esempio allorché sia utile per identificare il presunto autore del reato);
    - la sussistenza di motivi di sicurezza (es. rischio ambientale o altre situazioni di pericolo per la collettività);
    - quando sia necessario fornire informazioni oggettive sullo stato del procedimento penale al fine di prevenire turbative dell'ordine pubblico ovvero quando la diffusione di informazioni circa le modalità della condotta oggetto del procedimento penale sia utile a prevenire la commissione di ulteriori reati
c) Nel caso in cui la notizia sia già stata diffusa dagli organi di stampa e abbia assunto rilevanza pubblica, anche al di fuori dei casi di cui sopra, possono essere forniti alla stampa chiarimenti sullo stato del procedimento, al fine di consentire una corretta rappresentazione dei fatti ed evitare informazioni erronee, imprecise o distorte.

3. Tempistiche e modalità della comunicazione da parte dell'autorità giudiziaria

Per quanto possibile, i comunicati non possono essere pubblicati prima che gli interessati e/o i loro difensori abbiano ricevuto le notifiche dell'atto o, in caso di conclusione delle indagini, abbiano avuto l'opportunità in concreto di visionare gli atti. Le stesse regole valgono per la convocazione della conferenza stampa, che costituisce in ogni

caso un'eccezione.
La divulgazione di informazioni di cui ai punti a), b), c), deve essere operata, rispettando le previsioni degli artt. 329 e 114 c.p.p..
La comunicazione deve soddisfare le seguenti caratteristiche:

- imparzialità, chiarezza e sobrietà: deve essere chiarita la fase in cui il procedimento pende, precisando che si tratta di un'ipotesi investigativa provvisoria.
- l'attività deve essere attribuita in modo impersonale all'ufficio, escludendo ogni riferimento ai magistrati assegnatari del procedimento o agli operanti di PG che hanno partecipato ad atti di indagine;
- Deve essere assicurato il diritto dell'indagato/imputato a non essere indicato come colpevole fino a quando la colpevolezza non sia stata accertata con sentenza o decreto penale di condanna irrevocabili;
- essenzialità dell'informazione e sinteticità: salvo non sia assolutamente necessario ai fini della comunicazione, non devono essere riportati i nomi e le generalità delle persone (anche giuridiche), coinvolte (indagato, persona offesa, testimoni) o riferimenti che consentano di fatto di identificare l'indagato, né eventuali dati sensibili relativi a soggetti coinvolti nel procedimento (o di terzi).
- È vietato diffondere immagini di minori e di persone *in vinculis*.
- Nelle conferenze stampa, non è ammessa la proiezione di immagini, video né altre forme di rappresentazione ad uso comunicativo e/o esplicativo (garante privacy 18.5.2012)

In ogni caso, per garantire il rispetto della presunzione di innocenza e della dignità dei soggetti coinvolti, nonché del giusto processo e allo stesso tempo assicurare una informazione corretta, qualsiasi comunicazione relativa a procedimenti penali proveniente dall'Autorità Giudiziaria o dalla Polizia Giudiziaria (autorizzata dal Procuratore della Repubblica) deve essere fornita: *i)* limitandosi alle informazioni essenziali; *ii)* chiarendo la fase in cui il procedimento si trova e precisando che si tratta di un'ipotesi investigativa che deve essere verificata nel contraddittorio delle parti; *iii)* evitando espressioni enfatiche che possano in concreto indurre una considerazione dell'informazione data, che sia difforme rispetto ai principi qui condivisi.
Quando autorizza la pubblicazione di comunicati predisposti dalla Polizia Giudiziaria, la Procura deve sempre verificare che i contenuti di detti comunicati siano conformi alle indicazioni di cui al presente paragrafo, provvedendo, ove necessario, ad apportare le connesse modifiche e integrazioni.

4. Ordinanze applicative di misure cautelari personali e reali: presupposti per il rilascio di copia ai giornalisti e indicazioni redazionali.

Premesso che, nella vigenza dell'attuale normativa, i provvedimenti applicativi di misure cautelari personali e reali disposti dall'Autorità Giudiziaria non sono coperti da segreto o da divieto di pubblicazione (è però attualmente all'esame delle commissioni parlamentari lo schema di D. Lgs. di attuazione della legge di delegazione europea n.

15/24 – atto Governo n. 196 – che all'art. 2 ripristina il divieto di pubblicazione delle ordinanze custodiali), la valutazione circa la ricorrenza dei presupposti per la loro eventuale consegna alla stampa e ai *media* compete, senza alcun automatismo, alla medesima Autorità Giudiziaria.

Si conviene sul fatto che all'origine del divieto di pubblicazione degli atti di indagine di cui all'art. 114 co.2 c.p.p. sta il principio per il quale gli atti formati senza l'intervento della difesa siano, anche qualora sottoposti al vaglio del giudice, unilaterali e possano dunque essere compiutamente diffusi solo alla fine della fase di indagine se non addirittura dopo l'udienza preliminare. L'eventuale pubblicazione del contenuto degli atti non deve dunque superare il divieto in questione.

L'eventuale divieto di pubblicazione integrale o per estratto del documento è precetto che riguarda il giornalista il quale però, anche nell'interesse di una corretta e paritaria informazione, può avere la necessità del documento originario.

A tal fine, il Presidente del Tribunale adotterà tempestivamente un provvedimento autorizzativo con il quale – all'esito della esecuzione e della comunicazione a tutte le parti della misura adottata dal GIP o dal Tribunale - potrà autorizzare la trasmissione del provvedimento ai giornalisti accreditati e ad altri operatori della comunicazione che ne facciano richiesta, in presenza dei requisiti di cui all'art. 116 c.p.p., la cui ricorrenza verrà valutata anche sulla scorta del decalogo predisposto dall'Ordine dei Giornalisti allegato al presente documento.

In caso di diniego andranno esplicitati i motivi di non conformità rispetto a quanto concordato.

Il Procuratore potrà segnalare al Presidente del Tribunale la sussistenza di motivate esigenze investigative che ostino, anche temporaneamente, alla consegna del provvedimento ai giornalisti e ai media che ne abbiano fatto richiesta. In tal caso non si procederà alla consegna, salvo diverso avviso del Presidente, sentiti tempestivamente anche i soggetti processuali.

Nessun intervento, nemmeno di apposizione di *omissis*, verrà effettuato sul testo dei provvedimenti da parte del Presidente, potendo risultare comunque arbitrario in relazione alle differenti esigenze da tutelare.

La tutela dei terzi estranei al procedimento e l'attenzione verso la propalazione di dati ritenuti sensibili sono obiettivi da perseguire attraverso:

- una redazione del provvedimento che tenda ad escludere elementi non strettamente necessari per i fatti oggetto del tema procedimentale e per le necessità di motivazione del giudice:
- una informazione, applicativa anche del codice deontologico dei giornalisti e delle diverse Carte intervenute sulla tematica delle modalità di comunicazione in situazioni sensibili (da ultima Carta di Venezia), che puntualizzi sempre come il provvedimento adottato dal GIP si fondi esclusivamente sul materiale di prova raccolto nella fase delle indagini dal Pubblico Ministero in assenza di ogni interlocuzione con l'indagato e/o il suo difensore.

5. Informazione provvisoria e comunicati stampa

In relazione a procedimenti penali e civili di particolare interesse pubblico, individuati secondo i criteri enucleati nel paragrafo che precede, verranno adottate informazioni provvisorie di decisione o comunicazioni – secondo le linee guida del CSM – che possano fornire una informazione istituzionale, corretta, ufficiale.
In particolare per i processi penali definitivi ed in attesa del deposito delle motivazioni l'informazione provvisoria sarà adottata all'esito della camera di consiglio sentito il presidente del collegio o il giudice.

6. Il decalogo proposto dall'ordine dei giornalisti, ai fini dell'applicazione dell'art. 116 c.p.p.

Nelle richieste e nelle istanze, anche ai sensi dell'articolo 116 del codice di procedura penale, proposte dalla stampa agli organi giudiziari, può essere considerato sussistente un interesse ad acquisire copia degli atti che non siano coperti da segreto se, a livello nazionale o a livello locale:

- il crimine in questione è molto grave o ha caratteristiche tali da incidere nella quotidianità di una comunità, di una città o della vita civile nazionale, o nella visione del mondo dei lettori, anche sotto il profilo etico e di costume.
- c'è una connessione o una contraddizione tra un ufficio, un mandato, un ruolo sociale o una funzione anche professionale di una persona e l'azione per la quale è accusata, soprattutto - ma non solo - se le è richiesto il rispetto della credibilità, della fiducia dei cittadini e del decoro.
- c'è una connessione tra la posizione di una persona nota, anche a livello locale o in ambienti ristretti ma rilevanti per la vita sociale, e il crimine di cui è accusato oppure se il crimine di cui una persona è accusata è contraria alla sua immagine pubblica.
- un crimine grave è commesso in pubblico.
- è stato effettuato un arresto in flagranza.
- è stato emesso un mandato d'arresto o un fermo su iniziativa della polizia giudiziaria.
- in tutti gli altri casi in cui l'attenzione del pubblico abbia inequivocabilmente mostrato una solida rilevanza sociale e civile per il procedimento.
- in tutti quei casi dove l'azione del potere giudiziario limita la libertà personale dell'individuo e dunque è soggetta all'interesse giornalistico in funzione democratica, sia in fase di indagine preliminare sia in fase processuale, anche con specifico riferimento alla tutela della presunzione di innocenza nel processo penale.

Milano, 9 dicembre 2024
Il Presidente del Tribunale di Milano
Il Procuratore della Repubblica presso il Tribunale di Milano
Il Presidente dell'Ordine dei Giornalisti di Milano
Il Presidente dell'Ordine degli Avvocati di Milano
Il Presidente della Camera Penale di Milano

A proposito del dialogo tra giustizia e stampa: il tentativo del documento d'intesa milanese*

Alessia Forte

Abstract

Un approfondimento sul documento d'intesa in materia di informazione giudiziaria firmato presso il Tribunale di Milano, che pone al centro il difficile equilibrio tra il diritto a un'informazione completa e veritiera e la tutela della presunzione di innocenza.
An in-depth analysis of the agreement document on judicial information signed at the Court of Milan, which focuses on the difficult balance between the right to complete and truthful information and the protection of the presumption of innocence.

Sommario

Keywords

libertà di informazione – presunzione di innocenza – documento d'intesa in materia di informazione giudiziaria – interesse pubblico – accesso agli atti

1. Premessa

Il documento di intesa in materia di informazione giudiziaria, firmato il 9 dicembre 2024 presso il Tribunale di Milano dal suo Presidente, dal Procuratore della Repubblica di Milano, dal Presidente dell'Ordine degli avvocati di Milano, dalla Presidente della Camera Penale di Milano e dal Presidente dell'Ordine dei giornalisti, si propone quale

*Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

strumento di collaborazione che, partendo dal dato normativo, mira ad armonizzare il rispetto della presunzione di innocenza e il diritto-dovere ad un'informazione completa e veritiera.

A tal fine, come apertamente dichiarato nella parte introduttiva sulla genesi e sulle finalità del documento, il gruppo di lavoro si è posto l'obbiettivo di elaborare una serie di principi comuni e regole operative, in coerenza con quanto previsto, a livello normativo, dal decreto legislativo dell'8 novembre 2021, n. 188 e dal codice di procedura penale.

Resta estraneo al documento d'intesa l'ambito della diffusione illecita di atti coperti da segreto o per i quali sussista un divieto di pubblicazione (artt. 114 e 329 c.p.p.), per i quali è stato espressamente concordato che «le condotte in violazione delle norme penali (artt. 326 e 684 c.p.), salve le eventuali responsabilità in sede disciplinare, dovranno essere perseguite con assoluta fermezza e attivazione investigativa, nell'interesse delle persone coinvolte, del procedimento penale e del sistema dell'informazione».

Il documento non si presta ad uno statico riconoscimento di principi e regole condivise, ma assume l'obiettivo di evolvere costantemente attraverso il continuo perfezionamento del testo sottoscritto. A tale scopo, il gruppo di lavoro si impegna a proseguire nell'interlocuzione e nel monitoraggio dei comunicati emessi dalle autorità e delle conferenze stampa con l'eventuale indizione di incontri semestrali, su iniziativa di uno dei sottoscrittori. Da ultimo, si specifica che i principi condivisi verranno fatti oggetto di diffusione anche culturale da parte degli aderenti nei confronti di ogni soggetto terzo coinvolto, quali forze di polizia, personale amministrativo e cittadini.

2. Giustizia e informazione: una convivenza (im)possibile?

Il documento, per certi versi ambizioso, si colloca nel quadro del dibattito circa la convivenza tra la presunzione di innocenza – espressione privilegiata nel diritto sovranazionale in luogo della perifrasi negativa adottata dal testo costituzionale[1] – e il diritto dei cittadini ad un'informazione quanto più completa possibile, a piena realizzazione della libertà di manifestazione del pensiero quale «pietra angolare dell'ordinamento democratico»[2].

L'esigenza di una simile convivenza, definita non senza ragione «difficile, ma necessaria»[3], non emerge certo ora. Un magistrato, in tempi lontani, osservava come «giustizia e stampa, che in un'ideale isola di utopia, o in una felice Città del Sole sarebbero affettuose sorelle, concordemente affaccendate nella costante ricerca della verità, allo scopo di perseguire il bene comune e il castigo dei malvagi, sono invece, nel concreto

[1] Sul tema della distinzione tra le due locuzioni, si rinvia a P. Ferrua, *La prova nel processo penale*, I, *Struttura e procedimento*, Torino, 2017, 92 ss.

[2] Corte cost., 17 aprile 1969, n. 84.

[3] In questi termini N. Triggiani, *Introduzione. «E' la stampa, Bellezza! E tu non puoi farci niente! Niente!» (…Neppure con il soccorso della presunzione di innocenza),* in Id. (a cura di), *Informazione e giustizia penale*, Bari, 2022, 1.

del mondo in cui viviamo, naturalmente nemiche fra di loro»[4].
In effetti, sia la presunzione di innocenza sia la libertà di informazione costituiscono pilastri fondamentali dello Stato costituzionale di diritto che, in un mondo ideale, dovrebbero rafforzarsi vicendevolmente. Tuttavia, non è difficile rilevare l'esistenza di criticità[5] nel mantenere in equilibrio «due esigenze oggettivamente confliggenti»[6].
Questa conflittualità sprigiona tutta la sua forza soprattutto nel contesto dell'informazione giudiziaria che impone una serie di delicate valutazioni sul "se", "che cosa" e "come" pubblicare. In linea di principio, le notizie non dovrebbero essere veicolate in modo tale da suggerire nell'opinione pubblica convinzioni colpevoliste, non fondate sull'obiettivo materiale probatorio disponibile[7]. La verifica dell'ipotesi accusatoria[8], d'altronde, si afferma nel processo davanti ad un giudice terzo ed imparziale e non nel corso delle indagini preliminari, fase in cui tipicamente si concentra l'attenzione mediatica. Come è noto, il pubblico ministero – a prescindere dal controverso dovere espresso dall'art. 358 c.p.p., che prevede la necessità per il p.m. di svolgere accertamenti anche a favore della persona sottoposta alle indagini – tende a raccogliere solo una verità parziale, cioè di parte, senza il necessario apporto del contradditorio con chi potrebbe avere un alternativo punto di vista[9].
Al tempo stesso, però, la collettività deve essere posta nelle condizioni di potersi rappresentare una propria verità, che è il necessario frutto di un'attività informativa che talvolta supporta l'azione giudiziaria e talora la incalza, la critica e persino la scardina[10].
La circolazione ed il commento dei dati concernenti l'attività giudiziaria e i suoi esiti rispondono, infatti, a esigenze essenziali in una società democratica, ma ciò non toglie che debba essere ricercato un ragionevole contemperamento tra interessi contrappo-

---

[4] Così testualmente G. C. Romano Ricciotti, *Dal processo giudiziario al processo giornalistico*, in N. Lipari (a cura di), *Giustizia e informazione*, Roma-Bari, 1975, 272.

[5] Come puntualmente osserva P. Sammarco, *Giustizia e social media*, Bologna, 2019, 656.

[6] Così precisamente L. Ferrarella, *Non per dovere ma per interesse (dei cittadini): i magistrati e la paura di spiegarsi*, in *Questione giustizia*, 4, 2018, 310; Si noti, peraltro, come tale conflittualità emerga con chiarezza soprattutto nelle fonti sovranazionali. L'art. 19 del Patto internazionale sui diritti civili e politici specifica che la libertà di espressione può essere soggetta a limitazioni qualora ciò sia necessario, tra l'altro, per tutelare "il rispetto dei diritti o della reputazione altrui". In senso analogo e più ampio, l'art. 10 CEDU afferma che l'esercizio della libertà d'espressione "può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica [...] alla protezione della reputazione o dei diritti altrui".

[7] Cfr. F. Perchiunno, *Diritto all'informazione giudiziaria e altri interessi primari: un difficile bilanciamento*, in N. Lipari (a cura di), *Giustizia e informazione: dalla cronaca giudiziaria al "processo mediatico"*, cit., 81.

[8] Quanto meno quella processuale poiché, com'è noto soprattutto nella dottrina processualpenalistica, una società civile non può e non deve perseguire "ad ogni costo" la verità storica. Sul punto, si v., G. Giostra, *Prima lezione sulla giustizia penale*, Roma-Bari, 2020, 250 ss.

[9] Cfr. Unione Camere Penali, *La spettacolarizzazione dell'informazione giudiziaria oltre la presunzione di innocenza: un confine sempre più labile tra media e giusto processo, unione camere penali*, in *Osservatorio Informazione Giudiziaria, Media e Processo Penale*, 2024.

[10] A tal proposito, è utile sottolineare che la cronaca giudiziaria non necessariamente si pone in conflitto con gli interessi degli imputati: «la diffusione di informazioni sui processi permette all'opinione pubblica non solo di conoscere il fatto di reato e il suo autore, ma anche di controllare l'operato degli organi giurisdizionali, per evitare che essi, lontano da occhi indiscreti, abusino del proprio potere», come osservato da. C. Melzi d'Eril-G. E. Vigevani, *Informazione e giustizia*, in Aa. Vv. (a cura di), *Diritto dell'informazione e dei media*, Torino, 2022, 92.

sti[11].

In generale, si tratta di aspetti piuttosto noti, quasi scontati, anche perché i grandi processi penali, da quando esistono i giornali, hanno sempre suscitato l'attenzione dell'opinione pubblica, con conseguenti riflessi reputazionali sui diversi soggetti coinvolti.

Invece, ciò che è apparso come fenomeno degno di riflessione è che, in epoca attuale, si assiste ad un'amplificazione senza precedenti degli effetti derivanti dall'esposizione mediatica: l'informazione sul processo sta progressivamente lasciando spazio al c.d. «processo celebrato sui mezzi dell'informazione»[12], il quale, con una logica spesso bulimica, tende a captare – e talvolta a distorcere – ogni elemento disponibile, alimentando narrazioni fuorvianti[13]. In questo contesto, le notizie non vengono soltanto diffuse e discusse, ma si formano: il processo giudiziario ed i suoi protagonisti vengono valutati e giudicati in un'aula "virtuale" e da una giuria pubblica.

Si consideri, poi, che i processi celebrati sui mezzi dell'informazione (o, anche, "processi mediatici") procedono in parallelo ai processi ordinari, ma sono scanditi da due ritmi diversissimi: «da un lato, vi è l'"andatura" del processo, con i suoi tempi "geologici": la sentenza giunge di regola quando i *media* e la società hanno già da anni emesso la loro pronuncia e "archiviato" il fatto; dall'altro, vi è l'incalzante rapidità dell'informazione: la notizia è ormai prodotto effimero e i riflettori mediatici si possono attardare soltanto sulle primissime indagini»[14].

A complicare ulteriormente il quadro, interviene il peculiare meccanismo di funzionamento dei *social media* (ben distinto da quello dei *media* tradizionali): da un lato, esso consente a soggetti abitualmente estranei al mondo dell'informazione di diffondere "notizie", spesso frutto di ricostruzioni parziali e semplificate; dall'altro, alimenta con costanza il flusso telematico-informativo che si dipana in ogni angolo della rete, senza possibilità concreta di essere neutralizzato[15].

Di conseguenza, la compressione dei diritti fondamentali degli indagati e imputati, tra i quali rientra la presunzione di innocenza, appare oggi suscettibile di essere enormemente amplificata. Ciò con riguardo non solo alla dimensione spaziale, con le implicazioni già menzionate, ma anche a quella temporale: le informazioni, anche se false, sono ormai agevolmente reperibili per chiunque, anche a distanza di molti anni[16].

Ora, passate brevemente in rassegna le problematiche che incidono sui rapporti tra giustizia e informazione, occorrerà volgere un rapido sguardo alle soluzioni adottate

---

[11] Cfr. G. Mantovani, *Informazione, giustizia penale e diritti della persona*, Napoli, 2011, 3.

[12] G. Giostra, *Un catechismo per atei, Una prima lettura del d.lgs. n. 188 del 2021*, in questa *Rivista*, 2022, 5.

[13] G. Giostra, *Processo penale e mass media*, in *Criminalia – Annuario di scienze penalistiche*, 2007, 59.

[14] G. Giostra, *Un catechismo per atei*, cit., 11; In termini sostanzialmente analoghi L. Ferrarella, *Non per dovere ma per interesse (dei cittadini): i magistrati e la paura di spiegarsi,* cit., 310 in cui l'autore afferma l'esistenza di «tempistiche incompatibili» tra il processo mediatico e il processo ordinario, «tanto che proprio questa sfasatura di temi tra giustizia e suo racconto è tra le prime cause della disaffezione e dei pregiudizi dei cittadini»; Si v. anche C. Gabrielli, *Presunzione di innocenza e informazione giudiziaria*, in F. Cassibba-J. Della Torre-N. E. La Rocca-F. Zacchè (a cura di), *Le nuove frontiere della presunzione di innocenza*, Padova, 2024, 23.

[15] P. Sammarco, *La presunzione di innocenza. Un nuovo diritto della personalità*, Milano, 2022, 3, R. Orlandi, *La giustizia penale nel gioco di specchi dell'informazione, Regole processuali e rifrazioni deformanti*, in *Giustizia penale e informazione giudiziaria*, 3, 2017, 57.

[16] Cfr. Corte cost., 11 luglio 2021, n. 150.

sul piano normativo.

Già nel 1988 il legislatore, allo scopo di ricercare un equo bilanciamento tra gli interessi coinvolti, aveva tentato di dare una puntuale e articolata regolamentazione al tema del segreto investigativo e dei limiti alla pubblicazione degli atti di indagine attraverso gli artt. 114, 115 e 329 c.p.p. Questa regolamentazione, però, è stata immediatamente travolta da prassi devianti[17].

In tempi più recenti, la soluzione individuata prende le mosse dal d.lgs. 188/2021[18], e dal novellato art. 5 del decreto legislativo del 20 febbraio 2006, n. 106 in materia di rapporti con gli organi di informazione. Le innovazioni normative sono state animate dal perseguimento di un obiettivo condivisibile[19]: porre un freno ai deplorevoli giudizi anticipati di colpevolezza e agli eccessi di spettacolarizzazione delle inchieste giudiziarie[20].

Tuttavia, come vedremo, nonostante l'ottimo intendimento e il fondamentale passo in avanti compiuto sul terreno giuridico e culturale, le soluzioni adottate non si sono rivelate particolarmente soddisfacenti e in linea con gli obbiettivi dichiarati[21].

Ciò premesso, per meglio comprendere il contesto entro il quale il documento d'intesa intende esercitare i suoi effetti, giova richiamare brevemente il vigente quadro norma-

---

17 Messe ben in evidenza, fra i molti, da O. Mazza, *Tradimenti di un codice*, Torino, 2020, 55 ss.

18 Recante disposizioni per il compiuto adeguamento della normativa nazionale alle disposizioni della direttiva (UE) 2016/343 in tema di rafforzamento della presunzione di innocenza. Peraltro, si rileva che in attuazione della direttiva sono state adottate due deleghe legislative: la prima, con l. 25 ottobre 2017, n. 163, che il governo ha deciso di non esercitare, ritenendo che l'ordinamento giuridico nazionale contemplasse già garanzie adeguate e conformi alle disposizioni della Direttiva; la seconda (adottata a seguito della presentazione di una relazione sullo stato di attuazione della Direttiva), con l. 22 aprile 2021, n. 53, con la quale si perviene definitivamente all'emanazione del d.lgs. 8 novembre 2021, n. 188. In ogni caso, per una compiuta genesi del decreto legislativo, si v., fra i molti, N. Rossi, *Il diritto a non essere "additato" come colpevole prima del giudizio. La direttiva UE e il decreto legislativo in itinere,* in *Questione Giustizia*, 2021.

19 Ciononostante, è stato definito «improbo» da G. Giostra, *Comunicare il processo penale. Interessi costituzionali in precario equilibrio*, in C. Gabrielli (a cura di), *Comunicare il processo penale, regole, patologie, possibili rimedi*, cit., 17. Secondo l'autore, infatti, quando si tentano interventi sull'esercizio del diritto di informare e di essere informati «ci si incammina lungo un terreno scivolosissimo» e, infatti, tanto il legislatore italiano quanto quello europeo «hanno percorso pochissimi tratti in piedi».

20 F. Elisei, *Presunzione di innocenza: legge bavaglio o argine alla giustizia spettacolo?*, in C. Gabrielli (a cura di), *Comunicare il processo penale, regole, patologie, possibili rimedi*, cit., 72.

21 In proposito, in questa *Rivista* cfr. M. Castellaneta, *L'attuazione della direttiva sulla presunzione d'innocenza: atto dovuto o occasione per limitare la libertà di stampa?,* 1, 2022 e C. Melzi d'Eril, *Presunzione d'innocenza: un diritto leso, buone intenzioni, una disciplina inadeguata*, 1, 2022. Cfr. inoltre N. Triggiani, *Informazione e giustizia penale. Dalla cronaca giudiziaria al "processo mediatico*, in Id (a cura di), *Informazione e giustizia penale*, cit., 38; Alle medesime conclusioni perviene anche G.M. Baccari, *Le nuove norme sul rafforzamento della presunzione di innocenza, in Diritto penale e processo*, 2022, 2, 160; Analogamente si vedano anche le Note dell'Unione Camere Penali sullo "*Schema di decreto legislativo recante disposizioni per il compiuto adeguamento della normativa nazionale alle disposizioni della Direttiva UE 2016/343 sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali"*, in *Diritto di Difesa*, 2021, secondo cui lo strumento in commento risulterebbe «inidoneo a raggiungere lo scopo di mitigare uno dei fenomeni maggiormente distorsivi della presunzione di innocenza e del giusto processo». Invece, con riguardo alle critiche maturate sul fronte giornalistico, si v., a titolo d'esempio, le valutazioni del Presidente dell'Ordine dei Giornalisti della Lombardia, Riccardo Sorrentino, in occasione di un intervento tenuto nel corso di un incontro con l'ordine degli avvocati che si è svolto il 31 ottobre a Brescia sul tema dei *ritocchi degli articoli 114 e 116 del Codice di procedura penale e del disegno di legge in tema di presunzione di innocenza*, reperibile su *odg.mi.it*.

tivo, così come delineato dal d.lgs. 188/2021.

L'art. 2 del decreto ha inteso ridimensionare il perimetro comunicativo dell'autorità pubblica assegnando centralità al principio di non colpevolezza: viene, infatti, previsto il divieto per le autorità pubbliche[22] di indicare come colpevole la persona sottoposta ad indagini o l'imputato sino all'irrevocabilità della sentenza o del decreto penale di condanna. Tale prescrizione è assistita, oltre che da sanzioni di natura penale e disciplinare, dall'obbligo del risarcimento del danno derivante dalla lesione della presunzione di non colpevolezza e dal diritto per l'interessato di richiedere la rettifica della dichiarazione resa dall'autorità pubblica. Ove essa non venga disposta, ovvero non sia conforme alle stesse modalità della dichiarazione, l'interessato potrà rivolgersi direttamente al giudice a norma dell'art. 700 c.p.c.

Il successivo art. 3 ammette la diffusione di notizie sui procedimenti penali in corso solo se strettamente necessaria alla prosecuzione delle indagini o se giustificata da specifiche ragioni di interesse pubblico e unicamente per il tramite di comunicati ufficiali o, nei casi di particolare rilevanza, di conferenze stampa.

Infine, viene introdotto un apposito articolo 115 bis c.p.p. rubricato "garanzia della presunzione di innocenza" in base al quale "nei provvedimenti diversi da quelli volti alla decisione in merito alla responsabilità penale dell'imputato (…) l'autorità giudiziaria limita i riferimenti alla colpevolezza (…) alle sole indicazioni necessarie a soddisfare i presupposti, i requisiti e le altre condizioni richieste dalla legge per l'adozione del provvedimento".Sul piano deontologico-giornalistico, merita di essere segnalata la specifica norma posta a garanzia della presunzione di innocenza. Il Testo unico dei doveri del giornalista all'art. 8 recita "il giornalista rispetta sempre e comunque il diritto alla presunzione di non colpevolezza"[23]. Il linguaggio, chiaro e laconico, non lascia spazio ad alcuna interpretazione: la tutela dell'indagato e imputato trova, pertanto, una puntuale risposta sul piano deontologico, con la precisa assunzione di responsabilità da parte del giornalista.

---

[22] Nel declinare il divieto in questione, l'art. 2 richiama una nozione ampia di «autorità pubblica». La relazione illustrativa dello schema di decreto evidenzia la notevole latitudine della nozione che, come testualmente desumibile anche dal considerando 17 della direttiva, oltre alle autorità coinvolte nel procedimento penale, quali le autorità giudiziarie, di polizia e altre autorità preposte all'applicazione della legge, ricomprende qualsiasi altra autorità investita di potestà pubblicistiche quali ministri e altri funzionari pubblici. Ciò, conformemente all'ampia casistica emergente dalla disamina della giurisprudenza della Corte Edu. Per approfondimenti, si v. la relazione illustrativa dello schema di decreto legislativo recante *"Disposizioni per il compiuto adeguamento della normativa nazionale alle disposizioni della direttiva (UE) 2016/343 sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali"* su *giustizia.it*.

[23] Si segnala che l'attuale formulazione verrà a breve sostituita a seguito della recentissima approvazione del nuovo Codice deontologico da parte del Consiglio Nazionale dell'Ordine dei giornalisti. Il nuovo Codice, che entrerà in vigore il primo giugno 2025, prevede all'art. 24 (rubricato "Cronaca giudiziaria") che il giornalista «a) rispetta il diritto alla presunzione di non colpevolezza. In caso di assoluzione o proscioglimento, non appena informato, ne dà notizia con appropriato rilievo e adeguata tempestività; b) osserva la massima cautela nel diffondere nomi e immagini di persone accusate di reati minori o condannate a pene lievi, salvo i casi di particolare rilevanza sociale; c) si adopera affinchè risultino chiare le differenze fra documentazione e rappresentazione, fra cronaca e commento, fra indagato, imputato e condannato, fra pubblico ministero e giudice, fra accusa e difesa, fra carattere non definitivo e definitivo dei provvedimenti giudiziari, inquadrandoli nell'evoluzione delle fasi procedimentali e dei gradi di giudizio; d) garantisce adeguato spazio alle parti coinvolte in inchieste giudiziarie e processi».

3. Il documento d'intesa in materia di informazione giudiziaria: una collaborazione senza precedenti tra le diverse categorie professionali

Conclusa la premessa dell'attuale quadro dei rapporti tra presunzione di innocenza e informazione giudiziaria e venendo all'esame delle questioni sollevate dal documento d'intesa, preme anzitutto inquadrare il processo che ha portato alla sua formazione.
In primo luogo, la volontà di avviare un percorso comune per garantire una corretta rappresentazione delle vicende giudiziarie è emersa con evidenza, oltre che nel dibattito pubblico, anche nei vari momenti di confronto tra gli appartenenti alle diverse categorie coinvolte (*in primis* giornalisti, avvocati e magistrati). Questi incontri hanno fornito un fondamentale punto di riferimento nell'elaborazione documentale, non solo dal punto di vista contenutistico ma proprio di impostazione metodologica: l'apporto di soggetti qualificati appartenenti alle diverse categorie risulta, infatti, la modalità preferibile al fine di pervenire a conclusioni adeguate circa la complessità del tema affrontato[24].
Alla luce di tali considerazioni, nel giugno del 2023 è stato avviato un tavolo di discussione su iniziativa del Presidente del Tribunale di Milano che ha coinvolto anche l'Ordine dei giornalisti della Lombardia, la Procura di Milano, l'Ordine degli avvocati di Milano e, da ultimo, la Camera Penale di Milano, con il proposito di dar vita ad un documento condiviso sul delicatissimo tema della corretta informazione giudiziaria.
Il documento, frutto di un confronto definito dal Presidente dell'Ordine dei giornalisti della Lombardia «aperto e leale»[25], rappresenta un importante passo avanti nel tentativo di superare e, in qualche modo, "correggere" le rigidità imposte dal d.lgs. 188/2021.
Una simile metodologia rappresenta, a tutti gli effetti, un'innovazione in Italia nella sperimentazione regolativa dei rapporti tra uffici giudiziari, giornalisti e avvocati: in precedenza, infatti, si assisteva per lo più a protocolli operativi calati "dall'alto" da parte dei Tribunali, primi fra tutti quelli relativi all'individuazione di priorità nella trattazione degli affari penali.
Questo nuovo approccio partecipativo, al di là dei rilievi futuri allo stato impronosticabili, sembra accogliere positivamente l'auspicio che già nel 2018 il Consiglio Superiore della Magistratura aveva formulato in occasione di una delibera assunta sul tema della comunicazione istituzionale[26]. Infatti, in quella circostanza, l'organo di governo autonomo della magistratura sottolineava la necessità di sviluppare «forme appropriate di cooperazione» nei rapporti tra magistrati e *mass media.*
Non solo, l'iniziativa lombarda non si limita a fornire un modello locale, ma ambisce a diventare un punto di riferimento per l'intero territorio nazionale[27].

---

[24] Cfr. delibera del C.S.M., concernente le "Linee guida per l'organizzazione degli uffici giudiziari ai fini di una corretta comunicazione istituzionale" dell'11 luglio 2018.

[25] R. Sorrentino, *Il presunto colpevole non diventi chi deve informare*, in *Informazione e giustizia, dialogo di interesse pubblico*, New Tabloid – Periodico ufficiale del Consiglio dell'Ordine dei giornalisti della Lombardia, 2, 2024, 7.

[26] In questo senso, si v. delibera del C.S.M. concernente le "Linee-guida per l'organizzazione degli uffici giudiziari ai fini di una corretta comunicazione istituzionale" dell'11 luglio 2018.

[27] E. Fusco, *"Il nuovo protocollo sull'informazione giudiziaria firmata dal Tribunale di Milano, la Procura, L'Ordine*

Infatti, ad oggi non si registrano documenti analoghi in altri tribunali. L'unica iniziativa meritoria di menzione, per la quale non si può evidentemente parlare di "analogia" ma che condivide con quella lombarda gli intenti apprezzabili, è quella umbra del marzo 2022. In quell'occasione, è stato istituito in via sperimentale un osservatorio regionale permanente composto da giornalisti con il compito di monitorare, di concerto con la Procura generale di Perugia, la comunicazione ufficiale concernente procedimenti penali. Anche in questo caso l'obiettivo, stante l'esplicito riferimento alla volontà di migliorare la qualità dell'informazione giudiziaria, suole concretizzarsi attraverso l'avvio di un percorso comune tra giornalisti e Procure dal quale, però, a differenza dell'iniziativa lombarda, restano esclusi gli organi rappresentativi dell'avvocatura.

4. Verso una definizione "condivisa" di interesse pubblico

Una delle grandi discussioni che si sono aperte tra i vari soggetti partecipanti al gruppo di lavoro è quella riguardante la nozione di «interesse pubblico» e, in particolare, la minore o maggiore latitudine del concetto, posto alla base della comunicazione istituzionale delle Procure.

Sul punto, com'era presumibile, le opinioni si sono rivelate piuttosto polarizzate. In un primo momento, come dichiarato da uno dei protagonisti del gruppo di lavoro[28], la discussione ha persino rischiato di arenarsi definitivamente, a causa delle tensioni manifestatesi nella ricerca di un valido compromesso interpretativo.

Prevedibilmente, il momento di maggiore frizione si è manifestato tra inquirenti ed avvocati. Il problema, dal punto di vista degli avvocati, sarebbe il danno reputazionale dei cittadini coinvolti in un'inchiesta, in virtù del quale occorrerebbe rigidamente intendere il parametro-guida della comunicazione. All'opposto gli inquirenti, e ovviamente i giornalisti, si sono dimostrati favorevoli ad un approccio più ampio e flessibile nello scioglimento del nodo interpretativo.

Superata l'iniziale stasi, gli aderenti al gruppo di lavoro hanno inteso soffermarsi, con il precipuo intento di addivenire ad una definizione condivisa della nozione, sulla *ratio* dell'intervento riformatore.

Ma procediamo con ordine.

Come anticipato, l'art. 3 del d.lgs. 188/2021, che costituisce il cardine della normativa introdotta, interviene sul d.lgs. 106/2006 dedicato alla organizzazione degli uffici di Procura. In particolare, le modifiche si sono concentrate sull'art. 5 dedicato ai "rapporti con gli organi di informazione" incidendo sul *quomodo* della divulgazione delle informazioni circa procedimenti penali e, prima ancora, sull'*an*. Rinviando ad un secondo momento la trattazione delle modalità di diffusione delle informazioni (*quomodo*), ci si concentrerà prima di tutto sulle ragioni legittimanti la diffusione delle informazioni (*an*).

degli Avvocati, la Camera penale e l'Ordine dei giornalisti" che potrebbe diventare un riferimento per tutta Italia, Convegno *La rappresentazione mediatica dei processi: profili giuridici, linguistici e deontologici*, 16 gennaio 2025, Palazzo Reale Milano.

[28] R. Sorrentino, *Il presunto colpevole non diventi chi deve informare*, cit., 8.

Si prevede che la diffusione di informazioni sui procedimenti penali sia consentita esclusivamente al sussistere di un presupposto giustificativo per la comunicazione. Tale presupposto si ricaverebbe nella presenza di due condizioni tra loro alternative: una specifica esigenza investigativa oppure un rilevante interesse pubblico.

Orbene, all'indomani dell'entrata in vigore del decreto, le maggiori criticità si sono manifestate proprio in relazione al concetto di «interesse pubblico», posta l'evidente complessità di operare una precisa delimitazione del criterio, ritenuto particolarmente sfuggente. In particolare, ci si è chiesti come debba essere interpretato e se si debba far leva su un criterio modulato sul "tipo" di provvedimento oppure su una valutazione in concreto e caso per caso[29].

Un altro versante critico sarebbe poi rappresentato dal fatto che, nonostante l'apparente perentorietà della prescrizione («la diffusione di informazioni sui procedimenti penali è consentita *solo quando* (…)»), all'atto pratico, la divulgazione di informazioni riguardanti procedimenti penali dipenderebbe essenzialmente dalla discrezionalità di chi le detiene (cioè il p.m. titolare delle indagini), il quale ben potrebbe sostenere, a suo insindacabile giudizio[30], la ricorrenza del criterio[31]. Eppure, difficilmente contestabile appare l'affermazione che sia «sempre inoppugnabilmente sostenibile»[32] un interesse pubblico alla conoscenza o conoscibilità di un processo penale. In altre parole, ogni processo e ogni indagine rivestirebbe, per sua natura, un interesse pubblico e la segretezza non può che costituire un'eccezione, stabilita per rendere efficace l'azione investigativa[33].

Spostando l'attenzione sul fronte della disciplina europea, è facile notare come la norma italiana sembri ricalcare in maniera acritica il testo della direttiva[34], anch'essa poco nitida, di cui è attuazione[35]. Infatti, per meglio comprendere i termini dell'«interesse pubblico», in sede di confronto tra gli aderenti è parso opportuno esaminare anche

---

[29] A. Malacarne, *La presunzione di non colpevolezza nell'ambito del d.lgs. 8 novembre 2021, n. 188: breve sguardo d'insieme*, in *Sistema penale*, 2022.

[30] La tesi dell'insindacabilità è sostenuta, fra i molti, da G. Vigevani, *Riformare la riforma: le tre strade possibili,* in *Informazione, il tempo che fa: nuove strade e antiche minacce*, in *New Tabloid – Il periodico ufficiale dell'Ordine dei giornalisti della Lombardia*, 2, 2023, 29.

[31] Pertanto, secondo alcuni, in questo modo si cancella tutta d'un colpo la funzione di controllo della stampa sull'attività delle pubbliche autorità. Si v., in tal senso, il contributo di F. Elisei*, Presunzione di innocenza: legge bavaglio o argine alla giustizia spettacolo?*, cit., 74.

[32] L'espressione è di G. Giostra, *Presunzione di innocenza e tutela dell'immagine*, in F. Cassibba-J. Della Torre-N. E. La Rocca-F. Zacchè (a cura di), *Le nuove frontiere della presunzione di innocenza,* cit., 5.

[33] In questi termini, Ordine dei giornalisti della Lombardia, *Libertà di informazione*, 1, 2022, 5; Si v. anche, sul fronte europeo, la Raccomandazione (2010) n. 12 del Consiglio d'Europa, secondo cui «I procedimenti giudiziari e le questioni relative all'amministrazione della giustizia sono di pubblico interesse».

[34] Frutto, a sua volta, della «sintesi dei *dicta* in materia della Corte europea dei diritti dell'uomo», come osservato da C. Gabrielli, *Presunzione di innocenza e informazione giudiziaria*, in *Le nuove frontiere*, cit., 26.

[35] Infatti l'art. 4 della Direttiva, dopo aver specificato che "fino a quando la colpevolezza di un indagato o imputato non sia stata legalmente provata, le dichiarazioni pubbliche rilasciate da autorità pubbliche e le decisioni giudiziarie diverse da quelle sulla colpevolezza non devono presentare la persona come colpevole", afferma che le informazioni relative a determinati procedimenti penali possono comunque essere rilasciate dalle autorità pubbliche solo se ciò sia strettamente necessario per motivi connessi all'indagine penale o per l'interesse pubblico.

l'ambito di applicabilità della disciplina europea.

Così, a partire dalle disposizioni europee legittimanti la comunicazione delle Procure e nell'ambito della corretta individuazione della nozione di «interesse pubblico», si è convenuto di operare una sorta di separazione tra la comunicazione caratterizzante l'attività dei giornalisti e quella delle «autorità pubbliche»[36]. Solo nei confronti di quest'ultime si applicherebbe lo specifico parametro di cui al d.lgs. 188/2021 che presiede alla divulgazione delle informazioni sui procedimenti penali, come conferma la scelta del legislatore europeo di escludere dal campo di applicazione della direttiva i giornalisti[37] e come del resto dimostra il fatto che nel decreto legislativo l'attività giornalistica non è mai menzionata.

La ragione della non sovrapponibilità dell'interesse pubblico che deve improntare la comunicazione delle autorità pubbliche da quello che deve muovere l'attività giornalistica viene ricondotta alla diversità di ruolo e di funzioni che caratterizza le due figure: da un lato il giornalista che, in ragione della sua essenziale funzione di controllo dell'operato dei pubblici poteri, non può e non deve limitarsi ad una presa d'atto delle informazioni provenienti dall'ufficio requirente[38]; dall'altro il pubblico ministero che, in ragione della sua funzione istituzionale, è chiamato a rappresentare e tutelare gli interessi oggettivi dell'intero ordinamento giuridico[39].

Alla luce di queste considerazioni, il parametro legislativo cui devono riferirsi le autorità pubbliche non coincide con l'interesse pubblico che consente[40] ai giornalisti[41] di invocare, in sede sia civile che penale, l'esimente del diritto di cronaca in presenza di lesioni all'onore e alla reputazione di un individuo.

Infatti, mentre l'esercizio del diritto di cronaca deve essere il più ampio possibile, in conformità all'art. 21 della Costituzione, e può rispondere a criteri di rilevanza pubblica generale, la facoltà del Procuratore di divulgare informazioni su procedimenti penali è legata unicamente alle esigenze del procedimento penale e alla particolare gravità del fatto reato.

Fatte queste premesse, il documento procede a enumerare, senza pretesa di tassatività, i casi in cui è consentita la divulgazione di informazioni concernenti procedimenti

[36] Invero, sebbene il pubblico ministero risulti il principale destinatario dell'attenzione legislativa, l'art. 2 del decreto si rivolge alla più estesa platea "delle autorità pubbliche".

[37] Il Considerando 17, infatti, esplicita che per "dichiarazioni pubbliche rilasciate da autorità pubbliche" dovrebbe intendersi «qualsiasi dichiarazione riconducibile a un reato e proveniente da un'autorità coinvolta nel procedimento penale che ha ad oggetto tale reato, quali le autorità giudiziarie, di polizia e altre autorità preposte all'applicazione della legge, o da un'altra autorità pubblica, quali ministri e altri funzionari pubblici, fermo restando che ciò lascia impregiudicato il diritto nazionale in materia di immunità».

[38] In questo senso, si v. il contributo di G. Camera, *Cosa è di «interesse pubblico» in tema cronaca giudiziaria*, in odg.mi.it.

[39] F. Biondi-N. Zanon, *Il sistema costituzionale della magistratura*, Milano, 2024, 256.

[40] Congiuntamente al requisito della verità dei fatti esposti e della forma civile.

[41] Ma non solo: chiunque tramite, ad esempio, una semplice collaborazione occasionale con un periodico potrebbe, di fatto, esercitare l'attività giornalistica senza che gli sia richiesta l'iscrizione all'albo. Secondo la giurisprudenza di legittimità, infatti, è attività giornalistica qualunque "attività di lavoro intellettuale volta alla raccolta, al commento ed alla elaborazione di notizie destinate a formare oggetto di comunicazione interpersonale attraverso gli organi di informazione" (Cass. civ. sez. lav., 20 febbraio 1995, n. 1827).

penali, vale a dire: a) la sussistenza di motivi connessi all'indagine (ad esempio allorché sia utile per identificare il presunto autore del reato); b) la sussistenza di motivi di sicurezza (ad esempio in caso di rischio ambientale o di altre situazioni di pericolo per la collettività); c) quando sia necessario fornire informazioni oggettive sullo stato del procedimento penale al fine di prevenire turbative dell'ordine pubblico ovvero quando la diffusione circa le modalità della condotta oggetto del procedimento penale sia utile a evitare la commissione di ulteriori reati. Da ultimo, si specifica che anche al di fuori dei casi menzionati e nel caso in cui la notizia sia già stata diffusa dagli organi di stampa e abbia assunto rilevanza pubblica, possono essere forniti alla stampa chiarimenti sullo stato del procedimento.

Ciò detto, lo sforzo di individuare casi emblematici ove la sussistenza del pubblico interesse è già di per sé accertata, appare senz'altro lodevole. Per la verità, tale elenco nulla aggiunge allo stato dell'arte in quanto si limita a riprodurre pedissequamente quanto già affermato in sede europea[42]. In questo senso, sarebbe risultato preferibile ravvisare nuovi elementi da considerare in sede di valutazione della sussistenza dell'interesse pubblico, essendo quest'ultimo, come rilevato in precedenza, parametro di difficile interpretazione.

5. La comunicazione istituzionale da parte dell'autorità giudiziaria

Venendo ora alla trattazione delle modalità di diffusione delle informazioni circa procedimenti penali, l'art. 5 del d.lgs. 106/2006, nella formulazione precedente, si limitava a disporre, al primo comma, che il Procuratore della Repubblica mantiene i rapporti con gli organi di informazione personalmente o tramite delegato. Veniva, dunque, attribuita una notevole centralità al ruolo del Procuratore in qualità di unico soggetto legittimato ad intrattenere rapporti con gli organi dell'informazione, potendo al massimo avvalersi di un magistrato dell'ufficio appositamente delegato[43].

A seguito delle modifiche intervenute nel 2021 questa centralità viene rafforzata attraverso l'individuazione degli strumenti di comunicazione che possono essere a tal fine impiegati. Infatti, si prevede che la comunicazione debba avvenire esclusivamente tramite comunicati ufficiali oppure, nei casi di particolare rilevanza pubblica dei fatti,

[42] Invero, il considerando 18 della direttiva chiarisce già la casistica dell'interesse pubblico legittimante la comunicazione della Procura: «l'obbligo di non presentare gli indagati o imputati come colpevoli non dovrebbe impedire alle autorità pubbliche di divulgare informazioni sui procedimenti penali, qualora ciò sia strettamente necessario: per motivi connessi all'indagine penale, come nel caso in cui venga diffuso materiale video e si invita il pubblico a collaborare nell'individuazione del presunto autore del reato, o per l'interesse pubblico, come nel caso in cui, per motivi di sicurezza, agli abitanti di una zona interessata da un presunto reato ambientale siano fornite informazioni o la pubblica accusa o un'altra autorità competente fornisca informazioni oggettive sullo stato del procedimento penale al fine di prevenire turbative dell'ordine pubblico. Il ricorso a tali ragioni dovrebbe essere limitato a situazioni in cui ciò sia ragionevole e proporzionato, tenendo conto di tutti gli interessi. In ogni caso, le modalità e il contesto di divulgazione delle informazioni non dovrebbero dare l'impressione della colpevolezza dell'interessato prima che questa sia stata legalmente provata».

[43] C. Gabrielli, *Presunzione di innocenza e informazione giudiziaria*, in *Le nuove frontiere*, cit., 28.

tramite conferenze stampa[44]. Anche in questo caso, la formulazione ha disvelato significative criticità sintetizzabili nella considerazione che per contrastare la "cattiva" informazione (obiettivo che, in senso lato, si propone il decreto) risulterebbe maggiormente efficace focalizzare l'attenzione sulle modalità attraverso cui promuovere una corretta informazione, non certo sulla pretesa di ingessare le modalità di diffusione delle notizie[45].

Mettendo però da parte le questioni che attengono strettamente al dato normativo, è opportuno comprendere lo spazio d'intervento operativo del documento d'intesa riconducibile essenzialmente a due versanti, uno relativo alle tempistiche e uno relativo alle modalità.

In primo luogo, viene opportunamente prevista la non pubblicabilità dei comunicati prima che gli interessati e i loro difensori abbiano ricevuto le notifiche dell'atto o, in caso di conclusione delle indagini, abbiano avuto l'opportunità in concreto di visionare gli atti (indicazione valevole anche per la convocazione delle conferenze stampa). Ciò, come si vedrà più avanti, in coerenza con quanto sancito dall'art. 329 c.p.p. in tema di segreto investigativo.

In secondo luogo, viene stilato un elenco delle caratteristiche che devono improntare la comunicazione istituzionale, sia essa manifestata attraverso comunicati o conferenze stampa[46]. In realtà, l'elencazione si risolve in una mera riproduzione di norme previgenti dalla più svariata natura: basti pensare alla necessità di attribuire l'attività in modo impersonale all'ufficio escludendo ogni riferimento ai magistrati assegnatari del procedimento, contenuta nell'art. 5, comma 2, del d.lgs. 106/2006, all'esigenza di assicurare il diritto dell'indagato/imputato a non essere indicato come colpevole fino a sentenza o decreto penale di condanna irrevocabili, prevista dal successivo comma 2 bis, o al divieto di diffondere immagini di minori e di persone *in vinculis* stabilito dall'art. 114 commi 6 e 6 bis del c.p.p.

---

[44] Pertanto, devono ritenersi escluse tutte le modalità di diffusione delle informazioni diverse da quelle menzionate, tra le quali, a titolo d'esempio, colloqui informali, interviste alla stampa e dichiarazioni rese nel contesto di trasmissioni televisive. Sul punto, cfr. C. Gabrielli, *Presunzione di innocenza e informazione giudiziaria*, in *Le nuove frontiere*, cit., 28.

[45] Cfr. E. Bruti Liberati, *Delitti in prima pagina. La giustizia nella società dell'informazione*, Milano, 2022, 364; Alle medesime considerazioni pervengono anche C. Melzi d'Eril-G. E. Vigevani*, Informazione e giustizia*, cit., 85, secondo cui «per scongiurare ipotesi di comunicazione distonica rispetto alla presunzione di non colpevolezza, infatti, si pretenderebbe di inaridirne una delle fonti, in particolare quella della Procura, rispetto ai fatti di notevole interesse pubblico».

[46] Si riporta l'elenco completo contenuto nel documento: «a) imparzialità, chiarezza e sobrietà: deve essere chiarita la fase in cui il procedimento pende, precisando che si tratta di un'ipotesi investigativa provvisoria; b) l'attività deve essere attribuita in modo impersonale all'ufficio, escludendo ogni riferimento ai magistrati assegnatari del procedimento o agli operatori di polizia giudiziaria che hanno partecipato ad atti di indagine; c) deve essere assicurato il diritto dell'indagato/imputato a non essere indicato come colpevole fino a quando la colpevolezza non sia stata accertata con sentenza o decreto penale di condanna irrevocabili; e) essenzialità dell'informazione e sinteticità: salvo non sia assolutamente necessario ai fini della comunicazione, non devono essere riportati i nomi e le generalità delle persone (anche giuridiche), coinvolte (indagato, persona offesa, testimoni) o riferimenti che consentano di fatto di identificare l'indagato, né eventuali dati sensibili relativi a soggetti coinvolti nel procedimento (o di terzi); f) è vietato diffondere immagini di minori e di persone *in vinculis*. Nelle conferenze stampa, non è ammessa la proiezione di immagini, video né altre forme di rappresentazione ad uso comunicativo e/o esplicativo».

Certo è che non si poteva pretendere alcuna novità nell'enumerazione degli elementi ivi previsti, posta la valenza solo orientativa e non normativa di un simile documento. Pertanto, in questo caso, risulta apprezzabile lo sforzo ricognitivo degli aderenti al gruppo di lavoro nel guidare i protagonisti della comunicazione istituzionale.
Proseguendo nella disamina del documento, non può che rilevarsi il pregevole intento di soffermarsi anche sull'annosa questione dei presupposti per l'eventuale rilascio di copia ai giornalisti di ordinanze applicative di misure cautelari personali e reali disposte dall'autorità giudiziaria. L'intento, pur apprezzabile, è rimasto tale poiché, nel lasso di tempo intercorrente tra la pubblicazione del documento d'intesa e la stesura del presente contributo, è stato definitivamente approvato il decreto legislativo del 10 dicembre 2024, n. 198 con cui si prevede un nuovo adeguamento della normativa nazionale alle disposizioni europee sul rafforzamento della presunzione di innocenza.
L'intervento, risoltosi peraltro in un'unica disposizione di natura sostanziale, ha inteso modificare l'art. 114 c.p.p. con la definitiva consacrazione del divieto di pubblicazione delle ordinanze cautelari fin quando non siano concluse le indagini preliminari ovvero fino al termine dell'udienza preliminare[47]. L'effetto di tali modifiche, per quel che qui rileva, rischia di determinare il prematuro superamento delle previsioni operative espresse nel documento d'intesa.

6. Il decalogo volto a migliorare la previsione di accesso agli atti

Alla luce di quanto esaminato sinora, si rileva che il passaggio più significativo e maggiormente ambito dalla categoria giornalistica è rappresentato dal c.d. "decalogo ai fini dell'applicazione dell'art. 116 c.p.p.".
Procedendo con ordine, giova preliminarmente richiamare quanto previsto dalla disposizione processuale: quest'ultima, al primo comma, prevede la possibilità, riconosciuta a chiunque vi abbia interesse, di ottenere il rilascio a proprie spese di copie, estratti o certificati di singoli atti.
Gli atti ai quali si fa riferimento sono quelli per i quali sia venuto meno il segreto interno[48], quel segreto, cioè, finalizzato esclusivamente al buon esito dell'indagine (non alla dignità dell'imputato o alla riservatezza dei terzi), la cui regola fondamentale è espressa dal primo comma dell'art. 329 c.p.p. Tale disposizione prevede che gli atti investigativi della polizia e del pubblico ministero non siano accessibili ad altre persone, finché l'imputato o il suo difensore non ne possano avere conoscenza e, comunque, non oltre la chiusura delle indagini preliminari.
Una volta determinata la caducazione del segreto previsto dell'art. 329 c.p.p., chiunque vi abbia interesse può acquisire atti del procedimento. E, poiché, pacificamente, non

[47] Sul tema si rimanda al recentissimo contributo di A. Zampini, *Divieto di pubblicazione delle ordinanze che applicano misure cautelari personali: una scelta politica censurabile e costituzionalmente reprensibile*, in *Questione giustizia*, 2024.

[48] Per una disamina sulla distinzione tra segreto interno e segreto esterno si v., in particolare, F. Trapella, *La tutela del segreto investigativo*, in N. Triggiani (a cura di), *Informazione e giustizia penale*, cit., 166.

deve trattarsi di un interesse giuridicamente radicato nel procedimento *de quo*[49], anche il giornalista può chiedere ed ottenere l'accesso ad atti non più coperti da segreto interno. Attenzione, però, il fatto che il giornalista possa chiedere copia degli atti non significa che egli vanti un correlativo diritto a veder soddisfatta la sua richiesta: quest'ultima, infatti, ottiene riscontro mediante autorizzazione del pubblico ministero (art. 116, co. 2 c.p.p.), rendendo il giornalista di fatto dipendente dall'arbitraria valutazione dell'ufficio di Procura[50]. Infatti, si ravvisano prassi distorsive: il pubblico ministero tende a favorire determinati giornalisti – a proposito dei quali si è parlato di giornalisti "questuanti" – dando luogo ad una «censurabile "fiera delle informazioni" dagli esiti poco edificanti»[51]. Proprio su questo versante critico si incentrano le proposte, avanzate nel tempo da alcuni giornalisti[52] – per le quali si rileva il *favor* anche di parte del ceto magistratuale[53] – di disciplinare legislativamente il loro accesso agli atti, al fine di annichilire la dipendenza da fonti portatrici di interesse e, contestualmente, preservare la libertà e professionalità dei giornalisti. In altre parole, l'accesso al giornalista «eviterebbe di perpetuare situazioni di sostanziale sudditanza in cui egli può venire a trovarsi» e, soprattutto, «consentirebbe un esercizio realmente più responsabile dell'informazione»[54].

A tal proposito, le circolari di alcune procure[55] si sono spinte al punto di inserire a pieno titolo il giornalista tra i soggetti titolari di un interesse qualificato a richiedere copia di atti processuali non più segreti. In questo senso, non sono mancate critiche da parte della classe forense nelle quali si evidenzia l'insorgere del rischio di abbattimento dei principi sulla presunzione di innocenza[56].

Fatte queste premesse, occorre ora soffermarsi sulla soluzione individuata dagli aderenti al tavolo di confronto, in cui si è chiaramente tenuto conto delle istanze provenienti dalla classe forense.

---

[49] Cfr. P. Gaeta, *Il problema della divulgazione delle notizie giudiziarie*, in *Questione giustizia*, 2019.

[50] Cfr. G. Merlo, *Il segreto interno ed esterno e nuove prospettive per la pubblicazione degli atti,* in A. Camaiora-G. S. Bassi (a cura di), *Il processo mediatico*, *Informazione e giustizia penale tra diritto di cronaca e presunzione di non colpevolezza*, Padova, 2022., 71; C. Gabrielli, *Pubblico ministero, informazione giudiziaria e presunzione di non colpevolezza*, in *Questione giustizia*, la quale rileva l'esistenza di una certa resistenza culturale al riconoscimento di questo diritto quando a rivendicarlo sia un soggetto terzo rispetto al procedimento (come ad esempio il giornalista).

[51] R. Orlandi, *La giustizia penale nel gioco di specchi dell'informazione, Regole processuali e rifrazioni deformanti*, cit., 54.

[52] Spunti in tal senso in L. Ferrarella, *Il 'giro della morte': il giornalismo giudiziario tra prassi e norme*, in *Diritto penale contemporaneo - Rivista trimestrale*, 3, 2017 e, più di recente, Id., *Il "vorrei ma non posso" di un legislatore che "potrebbe ma non vuole"*, in questa *Rivista*, 1, 2018.

[53] Si veda, a titolo d'esempio, quanto espresso da A. Spadaro, *Commento al Decreto Legislativo 8 novembre 2021, n. 188*, in *Giustizia Insieme*, 2021.

[54] F. Palazzo, *Note sintetiche sul rapporto tra giustizia penale e informazione giudiziaria*, in *Diritto penale contemporaneo - Rivista trimestrale*, 3, 2017, 142; Cfr. anche E. Bruti Liberati, *Delitti in prima pagina*, cit., 255.

[55] In particolare, la Procura di Perugia che, nella circolare del 6 dicembre 2021, ha evidenziato la consapevolezza «che norme così rigorose potranno limitare il diritto degli operatori dell'informazione all'accesso alle notizie e persino, per una non voluta eterogenesi dei fini, incentivare la ricerca di esse attraverso canali diversi, non ufficiali o persino non legittimi» e ha individuato come possibile rimedio, l'accesso diretto dei giornalisti agli atti di indagine non più coperti da segreto, in linea con l'art. 116 c.p.p.

[56] Unione delle Camere Penali Italiane, *I principi di legge e le circolari di alcune Procure*, in *Osservatorio informazione giudiziaria media e processo penale,* 2022.

La proposta pervenuta dall'Ordine dei giornalisti, poi "recepita" dal tavolo di confronto, è stata quella di concedere al giornalista la possibilità di avanzare all'autorità giudiziaria una richiesta di accesso agli atti ogni qualvolta sia presente, a livello nazionale o locale, una delle seguenti situazioni: a) il crimine è molto grave o ha caratteristiche tali da incidere nella quotidianità di una comunità o nella visione del mondo dei lettori, anche sotto il profilo etico e di costume; b) c'è una connessione o una contraddizione tra un ufficio, un mandato, un ruolo sociale o una funzione anche professionale di una persona e l'azione per la quale è accusata; c) c'è una connessione tra la posizione di una persona nota, anche a livello locale o in ambienti ristretti ma rilevanti per la vita sociale, e il crimine di cui è accusato oppure se il crimine di cui una persona è accusata è contraria alla sua immagine pubblica; d) un crimine grave è commesso in pubblico; e) è stato effettuato un arresto in flagranza; f) è stato emesso un mandato d'arresto o un fermo su iniziativa della polizia giudiziaria; g) in tutti gli altri casi in cui l'attenzione del pubblico abbia inequivocabilmente mostrato una solida rilevanza sociale e civile per il procedimento; h) in tutti quei casi dove l'azione del potere giudiziario limita la libertà personale dell'individuo e dunque è soggetta all'interesse giornalistico in funzione democratica, sia in fase di indagine preliminare sia in fase processuale, anche con specifico riferimento alla tutela della presunzione di innocenza nel processo penale[57].
Si tratta di circostanze in cui è chiaramente ravvisabile un interesse pubblico alla conoscenza dei fatti e delle modalità di gestione da parte dell'autorità giudiziaria. Tuttavia, è fondamentale precisare che la possibilità di accedere agli atti in tali contesti non implica automaticamente un diritto incondizionato alla loro pubblicazione. Al fine di evitare responsabilità derivanti dalla diffusione delle informazioni, il giornalista è tenuto a conformarsi ai principi di verità, pertinenza e continenza espressiva, garantendo altresì il pieno rispetto del principio di presunzione di innocenza. In ogni caso, si tratta di aspetti puntualmente richiamati nelle norme deontologiche contenute sia nel Testo unico dei doveri del giornalista, sia nel nuovo Codice deontologico della categoria che entrerà ufficialmente in vigore nel giugno del 2025.

7. Qualche riflessione conclusiva

In conclusione, sembra certamente potersi apprezzare la modalità partecipativa impiegata dal documento milanese, a dimostrazione della reale volontà di creare sinergie virtuose tra categorie professionali tradizionalmente caratterizzate da posizioni divergenti.
Tuttavia, lo spazio d'intervento è severamente limitato in partenza. Le soluzioni suggerite incidono, ovviamente, a legislazione invariata poiché il fondamento di un simile documento è di natura "pattizia": si tratta di una sorta di *soft law*, di una regolamentazione che nasce dal basso. La conseguenza è che non ha, ne può avere, alcuna forza cogente sui singoli giornalisti, magistrati o avvocati, pur avendo inevitabili riflessi anche

[57] Il decalogo è stato stilato da un gruppo di lavoro di cui hanno fatto parte l'Avvocato Guido Camera, esperto di diritto dell'informazione, e Luca Rinaldi, giornalista di Milano Today e componente della Commissione Cronaca Giudiziaria dell'Ordine dei giornalisti della Lombardia.

su coloro i quali non vi hanno volontariamente aderito[58].

In ogni caso, le disposizioni contenute nel documento d'intesa, pur ricalcando in parte il controverso quadro normativo, offrono un'interpretazione estensiva delle modalità attraverso cui garantire una corretta rappresentazione delle vicende giudiziarie, lasciate normativamente nella disponibilità dei singoli magistrati.

Apprezzabile, nella direzione di un sistema comunicativo più equilibrato, appare soprattutto l'intento di soffermarsi sulla nozione di «interesse pubblico» e sull'individuazione di parametri oggettivi per l'accesso agli atti da parte della stampa. In entrambi i casi l'obbiettivo sullo sfondo è duplice: evitare tanto la spettacolarizzazione dei processi quanto l'oscuramento di informazioni di rilevante interesse pubblico.

Tuttavia, resta allo stato impronosticabile l'effettività dei principi espressi. Il contesto, costellato da prassi patologiche, certo non aiuta. Invero, se da un lato il documento d'intesa si propone come valido strumento di autodisciplina, dall'altro non si può ignorare la necessità di ulteriori interventi che rafforzino l'efficacia dell'impianto normativo, garantendo un più solido argine alle distorsioni del processo mediatico.

Ciononostante, il modello sperimentato a Milano potrebbe costituire un valido punto di riferimento per altre realtà territoriali, favorendo una più ampia riflessione a livello nazionale sul rapporto tra giustizia e informazione. La sua riuscita dipenderà non solo dall'impegno degli attori coinvolti nel rispettare le regole condivise, ma anche dalla capacità del sistema di recepire e valorizzare i principi espressi nel documento, trasformandoli in prassi consolidate e applicabili su larga scala.

[58] Cfr. L. Ciafardini, *Organizzazione degli uffici giudicanti e indipendenza funzionale del giudice*, in N. Zanon - F. Biondi (a cura di), *L'indipendenza della magistratura oggi*, Milano, 2020, 216.

Il documento di intesa in materia di informazione giudiziaria approvato a Milano: una sana iniezione di trasparenza

Giovanni Negri

Sommario

1. Una premessa speranzosa

Non è che ci volesse molto, eppure ci è voluto tanto. Tuttavia ora acquista maggiore concretezza la possibilità di una informazione giudiziaria, meglio di una cronaca giudiziaria, più efficace perché trasparente, meno condizionabile perché equilibrata. Il protocollo sull'accesso ai più delicati atti giudiziari, le ordinanze di custodia cautelare, sottoscritto a fine anno a Milano da tutti gli stakholders del processo penale, magistrati e avvocati in primo luogo, ma anche giornalisti come titolari del diritto a informare, è destinato a costituire un punto di riferimento. In netta controtendenza rispetto a un clima e a provvedimenti che dietro l'attrito tra diritto di cronaca ed esigenze di tutela della privacy si schermano per concretizzare misure che nel nome della seconda irragionevolmente comprimono il primo. Nulla di nuovo sotto il sole, naturalmente, visto che tra le più abusate, ma sempre ricorrenti, espressioni del dibattito, ad andare cauti, degli scontri, a essere più realisti, tra informazione e politica c'è quella proverbiale ormai di "legge bavaglio".

2. Un precedente partenopeo

Ora, il documento milanese ha molti meriti e qualche precedente. Quanto a questi ultimi, almeno da ricordare è l'ordine di servizio firmato dall'allora capo della Procura di Napoli Giovanni Melillo. Allora, si trattò di una decisione interna che, oltre a contribuire a disinnescare cortocircuiti sempre censurabili tra informazione e soggetti "a

conoscenza dei fatti" (giudici, Pm, forze dell'ordine, avvocati), andava nella direzione di quelle prassi virtuose di cui gli uffici del pubblico ministero allora erano stati protagonisti, basti pensare alla circolare di autoregolamentazione interna sulle intercettazioni e sui contenuti estranei al procedimento penale.
La leva giuridica utilizzata era quella dell'articolo 116 del Codice di procedura penale, in base al quale «durante il procedimento e dopo la sua definizione, chiunque vi abbia interesse può ottenere il rilascio a proprie spese di copie, estratti o certificati di singoli atti», nel perimetro del quale vengono riconosciti anche i giornalisti. Con particolare riferimento agli atti compiuti nella fase delle indagini preliminari per i quali è cessato l'obbligo di segretezza e, in particolare, i provvedimenti cautelari.
L'ordine di servizio di Melillo sottolineava di volere considerare il rilascio della copia funzionale al corretto esercizio del diritto di cronaca e all'interesse della pubblica opinione a essere correttamente informata. Nello stesso tempo, richiamando la necessità della valutazione del Procuratore sulla richiesta di accesso, ne fissava le condizioni. Il rilascio della copia, innanzitutto, non doveva interferire con le indagini in corso e piuttosto avvenire nel rispetto del principio di riservatezza; non doveva danneggiare i diritti dei soggetti coinvolti nel procedimento o di persone estranee; doveva avvenire, evitando la comunicazione di dati sensibili e la diffusione di notizie e immagini che potevano colpire la dignità delle vittime. Toccava comunque ai Procuratori segnalare, su indicazione dei titolari dei fascicoli, i provvedimenti giudiziari, non coperti da segreto, suscettibili di diffusione e relativi a casi di particolare gravità, delicatezza e rilevanza, insomma quelli di maggior interesse per l'informazione.

3. La storia del presente documento

Adesso, in un contesto normativo con significativi cambiamenti, primo tra i quali la direttiva sulla presunzione di innocenza e la sua disciplina di recepimento nell'ordinamento nazionale, è invece il tribunale di Milano a fare da punto di riferimento. È a Milano infatti che su iniziativa del presidente Fabio Roia, nella primavera 2023, è stato avviato un confronto che ha coinvolto sia gli operatori del diritto, magistrati (Tribunale e Procura) e avvocati (Ordine forense e Camere penali) sia i professionisti dell'informazione con l'intervento del locale Ordine dei giornalisti.
L'intenzione, dichiarata e condivisa dal gruppo di lavoro, è stata quella di coniugare presunzione di innocenza e corretta e completa informazione, attraverso l'elaborazione di principi comuni e regole operative. Espressamente estraneo al perimetro di applicabilità del protocollo è l'ambito della diffusione illecita di atti coperti da segreto o per i quali esiste divieto di pubblicazione; "in entrambi i casi, si concorda che le condotte in violazione delle norme penali (articoli 326 e 684 del Codice penale), fatte salve le eventuali responsabilità disciplinari, dovranno essere perseguite con assoluta fermezza e attivazione investigativa, nell'interesse delle persone coinvolte, del procedimento penale e del sistema dell'informazione tutto".

4. La nozione di interesse pubblico e l'accesso alle ordinanze di custodia cautelare

Due le conclusioni condivise raggiunte dal gruppo di lavoro su altrettanti punti cruciali dell'informazione giudiziaria: la nozione di interesse pubblico cui il decreto di recepimento della direttiva sulla presunzione d'innocenza àncora la comunicazione delle Procure e l'accesso alle ordinanze di custodia cautelare e agli atti a queste equiparabili. Sul primo, l'interesse pubblico che consente al Procuratore della Repubblica di divulgare informazioni sui procedimenti penali (o di autorizzare la Polizia Giudiziaria a fornire informazioni tramite comunicati stampa) è strettamente connesso alle esigenze del procedimento penale o alla particolare gravità del reato. Per esempio, si è convenuto di individuare l'esistenza di un interesse pubblico per motivi di sicurezza (è il caso per esempio del rischio ambientale o di altre situazioni di pericolo per la collettività); quando è necessario fornire informazioni oggettive sullo stato del procedimento penale per ragioni di ordine pubblico oppure per ragioni di prevenzione di altri reati. A mo' di norma di chiusura, quando la notizia è già stata diffusa e ha assunto rilevanza pubblica, possono essere forniti ai giornalisti chiarimenti sullo stato del procedimento, per consentire una corretta rappresentazione dei fatti ed evitare informazioni erronee, imprecise o distorte.
Sulla determinazione invece dell'interesse dell'informazione all'accesso agli atti, sulla base dell'articolo 116 del Codice di procedura penale, del protocollo fa parte anche un dettagliato elenco messo a punto dall'Ordine dei giornalisti che lo considera esistente quando:

- il crimine in questione è molto grave o ha caratteristiche tali da incidere nella quotidianità di una comunità, di una città o della vita civile nazionale, o nella visione del mondo dei lettori, anche sotto il profilo etico e di costume;
- c'è una connessione o una contraddizione tra un ufficio, un mandato, un ruolo sociale o una funzione anche professionale di una persona e l'azione per la quale è accusata, soprattutto - ma non solo - se le è richiesto il rispetto della credibilità, della fiducia dei cittadini e del decoro;
- c'è una connessione tra la posizione di una persona nota, anche a livello locale o in ambienti ristretti ma rilevanti per la vita sociale, e il crimine di cui è accusato oppure se il crimine di cui una persona è accusata è contraria alla sua immagine pubblica;
- un crimine grave è commesso in pubblico;
- è stato effettuato un arresto in flagranza;
- è stato emesso un mandato d'arresto o un fermo su iniziativa della polizia giudiziaria;
- in tutti gli altri casi in cui l'attenzione del pubblico abbia inequivocabilmente mostrato una solida rilevanza sociale e civile per il procedimento;
- in tutti quei casi dove l'azione del potere giudiziario limita la libertà personale dell'individuo e dunque è soggetta all'interesse giornalistico in funzione democratica, sia in fase di indagine preliminare sia in fase processuale, anche con specifico riferimento alla tutela della presunzione di innocenza nel processo penale.

5. Il provvedimento attuativo della Procura e il recente divieto di pubblicazione delle ordinanze cautelari

A valle del protocollo, il presidente Roia ha poi diffuso un provvedimento attuativo del protocollo che da una parte, in sintonia con le Linee guida del Csm sulla comunicazione istituzionale degli uffici giudiziari, prevede l'emanazione di un'informazione provvisoria con chiarimenti puntuali quando il solo dispositivo della decisione non è di facile lettura, dall'altra, nel caso di adozione di misure cautelari e (non solo quelle personali ma anche quelle reali) e se esiste un interesse alla diffusione nei termini delineati dal protocollo autorizza il rilascio di copia del provvedimento al giornalista interessato. Alla richiesta potrà rispondere la stessa presidenza del Tribunale oppure, su delega, quella dell'ufficio Gip-Gup.
Più che una semplice suggestione provocata dalla coincidenza cronologica è poi il sovrapporsi degli esiti del tavolo di confronto milanese alla definitiva approvazione da parte di Governo e maggioranza della disciplina di rafforzamento della presunzione d'innocenza, cristallizzata nell'istituzione di un divieto di pubblicazione, in nulla imposto da vincoli comunitari peraltro come precisato dal commissario europeo alla Giustizia Michael McGrath in risposta a un'interrogazione, del testo integrale o anche solo di estratti delle ordinanze che dispongono misure cautelari personali.

6. Un giudizio complessivo sul Protocollo

Il protocollo e le misure attuative di Milano non sono inconsapevoli del nuovo quadro normativo e tuttavia sposano una posizione condivisibile, nel segno della responsabilizzazione degli organi di informazione: in sostanza il divieto di pubblicazione non compromette il diritto a potere disporre dell'atto integrale sul quale esercitare, nei modi voluti dal legislatore, la cronaca giornalistica.
Una sommessa conclusione allora: se ha un merito la via ambrosiana alla identificazione di un percorso che tenga insieme con la minore forza conflittuale interessi e posizioni anche divergenti tra i protagonisti dell'informazione giudiziaria è di contribuire ad attenuare alcune delle storture evidenziate dall'affermarsi del modello mediatico di processo penale. La libertà di accesso agli atti giudiziari non più coperti da segreto, nella trasparenza, con regole chiare, è una forma di garanzia per tutti e anche una maniera per potere controllare e rendere informata l'opinione pubblica dell'attività della magistratura, in una stagione in cui il recupero di credibilità non può che passare anche dal confronto con il diritto di cronaca.

The use of AI in electoral campaigns: key issues and remedies*

Giuseppe Muto

Abstract

The expanding influence of artificial intelligence in electoral campaigns presents substantial challenges, particularly as it becomes a tool for generating and propagating disinformation, thereby undermining democratic principles. The following observations relate to the legal frameworks of the United States and the European Union that address such concerns. Within the United States, the utilization of artificial intelligence for the manipulation of public opinion has given rise to reinterpretations of the First Amendment, whereas the European Union has introduced legislative reforms. Alongside these normative developments, the paper also considers the initiatives undertaken by major private sector entities, such as Google and Meta, to prevent the misuse of AI technologies in political advertising and the dissemination of false information. It argues for a comprehensive approach – encompassing legislative measures, regulatory oversight, and private sector cooperation – to protect electoral integrity and uphold democratic values in the digital era.

Il crescente sfruttamento dell'intelligenza artificiale nelle campagne elettorali pone sfide significative, soprattutto per la sua capacità di creare e diffondere disinformazione. Ciò mette a rischio i principi democratici. Queste brevi note descrivono gli atti normativi adottati dagli Stati Uniti e dall'Unione Europea per affrontare tali problematiche. Negli Stati Uniti, la manipolazione dell'opinione pubblica mediante l'uso dell'IA sta conducendo a nuove interpretazioni del Primo emendamento, mentre nell'Unione Europea sono state introdotte norme specifiche per contrastare il fenomeno. L'analisi considera, inoltre, le iniziative intraprese dai grandi attori del settore privato, come Google e Meta, volte ad arginare l'uso improprio delle tecnologie di IA nella pubblicità politica e nella diffusione delle notizie. Emerge la necessità di un approccio articolato che integri misure legislative, regolatorie e la cooperazione del settore privato, al fine di salvaguardare l'integrità elettorale e i valori democratici nell'era digitale.

* This text incorporates, with necessary modifications, the discussions held during a panel orga-nized within the ICON•S Annual Conference, which took place in Madrid from 8 to 10 July 2024.

Summary

Keywords

elections – AI – democracy – disinformation – European Union

1. Introduction

2024 was the year of elections.[1] In that year, countries home to nearly half of the world's population held elections, marking a first in history. These include seven of the world's ten most populous nations: Bangladesh, India, the United States, Indonesia, Pakistan, Russia, Mexico and the European Union. Within concerns about the decline of democracies worldwide, these elections represented a crucial year for democracy itself. Despite threats to democracy, such as increased ethnic violence and attempts to weaken judicial checks on executive power, the popularity of democracy remains high. In this unstable context, generative AI represented a novel challenge in this historic election year.

It has become clear that artificial intelligence have played an increasing role in the production of disinformation and manipulation of information, an issue that had been relevant in that pivotal year for democracy.[2] Evidence from Newsguard, a database that collects and catalogues false information on the web, demonstrates a concerning trend: in the period between 1 January 2021 and 30 May 2024, Newsguard had identified that 5.48% of false information was produced by means of AI. This percentage is particularly concerning given the sharp rise over a relatively short period: in 2021, only 0.78% of false information was attributed to AI, and this figure had risen to 8.5% by 2024.[3]

[1] S. Shamim – A. Lodhi, *The year of elections – Is 2024 democracy's biggest test ever?*, in *aljazeera.com*, 4 January 2024.

[2] C. Vaccari – A. Chadwick, *Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News*, in *Social Media + Society*, 6, 1, 2020.

[3] More information is available here at *newsguardtech.com*. On this topic, see O. Pollicino, *Disinformazione e intelligenza artificiale: un cocktail esplosivo?*, in *Rivista della Corte dei Conti*, *forthcoming*.

2. AI, disinformation and the world outside the window

The proliferation of disinformation necessitated heightened attention, particularly in the context of crucial democratic functions. This is not merely an abstract concern, but a matter of demonstrable harm. Disinformation campaigns can be used to manipulate public opinion, undermine trust in legitimate institutions, and sow discord among citizens. These effects can have a direct and detrimental impact on elections, referendums, and other democratic processes.[4] A pertinent example is provided by the recent annulment of the presidential elections in Romania. In light of allegations of foreign interference, particularly from Russia, involving both disinformation and misinformation, the Romanian Constitutional Court's decision to invalidate the first round of elections has ignited considerable debate regarding the ramifications for democratic governance.[5] Critics argue that this ruling not only undermines the voices of millions of voters but also raises critical questions about the role of the judiciary in electoral processes.[6] This issue of constitutional relevance highlights the delicate balance that must be maintained to protect democratic principles while ensuring the integrity of elections, emphasizing the need for transparent mechanisms that safeguard both electoral outcomes and fundamental freedoms.

Therefore, the interplay between disinformation and democratic processes takes on heightened significance within the current geopolitical climate, characterized by ongoing international conflicts, particularly in Russia and the Middle East. In such an environment, disinformation can be weaponized to exacerbate existing tensions, destabilize fragile governments, and even serve as a precursor to armed conflict.[7] For example, malicious actors may use disinformation to create a false narrative justifying military intervention, or disrupt diplomatic efforts.[8]

Artificial intelligence has emerged as a potent weapon in the arsenals of modern warfare, surpassing its role in simply enhancing the precision of traditional weaponry. Often operating with minimal human oversight, AI-powered autonomous weapon systems (AWS) raise a multitude of legal and ethical concerns regarding proportionality, accountability, and the blurring of lines between combatants and civilians.[9] Furthermore, AI serves as a formidable tool for both domestic and international propaganda campaigns. State actors demonstrably utilize deepfakes, face swaps, lip-syncing, text-to-speech, and voice conversion to fabricate narratives that diverge significantly

[4] M. Kelly – E. Samuels, *How Russia weaponized social media, got caught and escaped consequences*, in *washingtonpost.com*, 18 November 2019.

[5] A. L. Solea, *Why Romania's election was annulled – and what happens next?*, in *The Conversation*, 16 December 2024

[6] A. Carrozzini, *Shooting Democracy in the Foot?*, in *Verfassungsblog*, 13 December 2024.

[7] See A.R. Di Maggio, *Fake News as Propaganda: The Bush and Obama Years*, in *Fake News in America: Contested Meanings in the Post-Truth Era*, Cambridge, 2023.

[8] J. Buchheim – G. Abiri, *The War in Ukraine, Fake News, and the Digital Epistemic Divide*, in *verfassungsblog.de*, 12 May 2022.

[9] It is not a case that Pope Francis during the session of G7 in Apulia concerning AI claimed that «no machine should choose to take the life of a human being», as reported by S. Cernuzio, *G7, il Papa: nessuna macchina dovrebbe scegliere se togliere la vita a un essere umano*, in *vaticannews.va*, 14 June 2024.

from reality.[10] A prime illustration of this is the now-debunked video, released in February 2022, purporting to show Ukrainian President Volodymyr Zelensky urging his citizens to give up.[11]

The nexus between AI-fueled disinformation, foreign propaganda, and the manipulation of democratic processes has been demonstrably established, even in relatively peaceful periods. For instance, in 2022, a group of British Members of Parliament lodged a complaint with the European Court of Human Rights against the Russian Federation.[12] Their claim centered on alleged violations of art. 3 of the First Additional Protocol to the European Convention on Human Rights (the right to free elections)[13], since they argued that Russia employed a sophisticated AI-powered disinformation campaign to influence the outcomes of the 2014 Scottish independence referendum, the 2016 Brexit referendum, and the 2019 UK general election. These campaigns reportedly involved the use of deepfakes, social media bots, and targeted online advertising to spread misinformation, sow discord, and erode public trust in democratic institutions.[14] Similarly, in the United States, many reports detailed extensive evidence of Russian interference in the 2016 presidential election, with suspected use of AI-powered tactics to manipulate social media algorithms and target swing voters with misleading content.[15] In these particular instances, AI has been utilised as a social bot or as a potent instrument for the organisation of online content. Social bots, which are essentially counterfeit accounts managed either automatically or semi-automatically, have the objective of disseminating material of a "polluting" nature. Moreover, AI assumes a significant role in the content recommendation systems that are present on the feeds of various platforms, playing a fundamental role in the propagation of information and the shaping of public consciousness. They have the capacity to influence and structure user preferences, guiding decisions at both the individual and collective levels, with a particular emphasis on political choices. This underscores the profound impact that AI has on our digital society.

Hence, considering the significantly deteriorated geopolitical framework compared to the past when such interference occurred, it appears necessary and fitting to adopt

[10] For an deepen analysis of the different type of deepfakes, consider O. Pollicino – P. Dunn, *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi (ed opportunità)*, in *federalismi.it*, 12, 2024.

[11] M. Holroyd, *Deepfake Zelensky surrender video is the 'first intentionally used' in Ukraine war*, in *euronews.com*, 16 March 2022.

[12] ECtHR, *Bradshaw et al v. Regno Unito*, app. 15653/22 (2022).

[13] Art. 3 of the First Additional Protocol to the European Convention on Human Rights, according to which «Right to free elections. The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature».

[14] J. Grierson, *MPs take Russian election interference case to human rights court*, in *theguardian.com*, 29 March 2022.

[15] Among the others, M. Rodriguez, *Disinformation Operations Aimed at (Democratic) Elections in the Context of Public International Law: The Conduct of the Internet Research Agency During the 2016 US Presidential Election*, in *International Journal of Legal Information*, 47, 3, 2019. On the same point, see also *(U)Report of the Select Committee on Intelligence United States Senate on Russian Active Measure Campaigns and Interference in the 2016 U.S. Election*, available at intelligence.senate.gov; S. Lynch, *U.S. Justice Dept. asks watchdog to check for political motivations in FBI Russia probe*, in *reuters.com*, 21 May 2018.

suitable measures to ensure the free and fair conduct of electoral competitions in this 'super' election year. The most crucial challenge confronting legislators on both sides of the Atlantic is to discern the thin line that separates a justified and reasonable restriction on freedom of expression from detestable censorship. This task, while delicate, is of utmost importance in preserving the integrity of our democratic processes.[16] Indeed, the ongoing war in Ukraine, appropriately labeled the «first social media war»[17], has presented a unique challenge in balancing freedom of expression with the need to counter foreign disinformation. This tension appears to have been recognized by the Tribunal of the European Union.[18] In a landmark case, the Tribunal upheld the legitimacy of sanctions imposed on a French television channel that broadcasted Russian propaganda messages. The Tribunal justification rested on the principle of proportionality – the restriction on the channel's freedom of expression was deemed necessary to counteract a significant threat posed by foreign disinformation. This decision finds its constitutional foundation in the principles expressed in the Charter of Fundamental Rights of the Union, that provide a legal framework for navigating the complex interplay between free speech and the need to combat information manipulation in the digital age.[19]

3. The USA

3.1. A new reading of the First Amendment

In response to the increasing power and influence of AI tools, both the United States and the European Union implemented a range of measures to prevent the exploitation of these technologies in the context of the 2024 elections.
The non-regulation approach, which generally characterises the US's style to digital regulation, has, allegedly, led to unauthorised influences on the 2017 election results. This has highlighted the need for «a narrow law prohibiting the use of AI to deceptively undermine our elections through fake speech».[20] While the First Amendment[21] safeguards the «free marketplace of ideas»,[22] it cannot be construed as providing con-

[16] On this topic, see O. Pollicino, *General Report: Freedom of Speech and the Regulation of Fake News*, in O. Pollicino (edited by), *Freedom of Speech and the Regulation of Fake News*, Cambridge, 2023; G. Pitruzzella, O. Pollicino, *Disinformation and Hate Speech: A European Constitutional Perspective*, Milan, 2020.

[17] P. Suciu, *Is Russia's Invasion Of Ukraine The Firs Social Media War?*, in *Forbes*, 1 March 2022.

[18] GC, T-125/22, *RT France v. Council* (2022).

[19] P. Dunn, *Il contrasto europeo alla disinformazione nel contesto della guerra in Ucraina: riflessioni a margine del caso* RT France, in *Rivista di diritto dei media*, 1, 2023.

[20] Congress of the United States of America - Senate Rules and Administration, S.Hrg. 118-130 – AI and the Future of our Elections, 27 September 2023.

[21] Constitution of the United States of America, First Amendment: «Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances».

[22] This definition was elaborated in a 1997 judgement of the American Supreme Court (*Reno v. Aclu*, 521 US 844 (1997)), recalling a famous expression formulated in the very important dissenting opinion

stitutional protection for those who intentionally defraud voters.

3.2. Who has the legitimacy for the protection of free elections?

It may be argued that the Federal Election Commission (FEC) possesses the legislative legitimacy to enact a regulation that restricts the use of certain AI tools during elections. This regulation, to be enforceable, would need to survive judicial review under the strict scrutiny test[23] established by the Supreme Court. This test is the most demanding standard applied by courts to evaluate restrictions on First Amendment rights. To pass this test, the FEC would need to demonstrate that the regulation is narrowly tailored to achieve a compelling governmental interest. In this case, the compelling interest would be safeguarding the integrity of the electoral process from being undermined by AI-powered tools capable of generating entirely fabricated realities and convincing voters. In this context, the forthcoming judgments of the Supreme Court in the TikTok case may offer crucial insights into the limitations of governmental authority to restrict access to digital platforms under the First Amendment.[24]
Therefore, the FEC, as the federal agency tasked with overseeing campaign finance and election administration, seems to be well-positioned to craft regulations that address this specific threat. However, this approach also faces challenges.[25] Indeed, in a recent statement,[26] the FEC clarified that while it lacks the authority to create new regulations specifically targeting AI,[27] the current provisions of the Federal Election Campaign Act (FECA) are applicable to deceptive AI-generated communications. This acknowledgment came after a petition from Public Citizen, which sought clarification on how these laws pertain to AI-generated ads. The FEC's interpretation indicates that any AI-generated content that constitutes fraudulent misrepresentation, as defined under FECA, is already prohibited by existing regulations. However, the agency emphasized that not all AI-generated content is inherently misleading, and it cannot regulate de-

of Justice Holmes in 1919 (*Abrams v. United States*, 250 US 616 (1919).

23 Among the others, R.H. Fallon, *Strict Judicial Scrutiny*, in *UCLA Law Review*, 54, 1267, 2007.

24 The recent ruling by the Court of Appeals for the D.C. Circuit in the TikTok case (*TikTok Inc. v. Garland*, No. 24-1113 (D.C. Cir. 2024)) marks a pivotal moment in the ongoing debate over the regulation of digital platforms and the application of strict scrutiny regarding freedom of expression. The court upheld the constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act, which imposes a ban on TikTok in the United States, asserting that the law does not violate the First Amendment or the equal protection rights guaranteed by the Fifth Amendment. This case is now subject to expedited appeal before the Supreme Court, where it will be determined whether the scope of strict scrutiny may be significantly reduced. Such an outcome could have profound implications for online free speech and the government's authority to restrict access to foreign platforms.

25 D. Young – J. Gardner – M. Block, *FEC Interpretive Rule on AI in Political Ads*, in *Policy Backgrounders*, 25 September 2024.

26 Federal Election Commission, *Concurring Statement of Chairman Sean J. Cooksey on Notification of Disposition of Reg 2023-02: Artificial Intelligence in Campaign Ads*, 19 September 2024, available at *fec.gov*.

27 C. Mcisaac, *FEC Makes the Right Call on AI Regulation in Federal Elections*, in *R Street Institute*, 16 September 2024.

ceptive practices beyond the narrow confines of the law as it currently stands.

4. The European Union

On the other side of the Atlantic, in Europe, there has been a growing recognition of the need to address the shortcomings of the 2018 Code of Practice on Disinformation. This Code was found to be disappointing due to its over-reliance on self-regulation, a trait it shares with the regulatory approach in the United States. This excessive dependence on self-regulation has been identified as a weakness, as it often fails to adequately address the complex and evolving challenges posed by disinformation.
Consequently, the EU has implemented a diverse set of tools specifically designed to counteract the malicious use of artificial intelligence during elections. These measures aim to provide a more comprehensive and proactive response to disinformation, surpassing the constraints inherent to self-regulation.

4.1. The Action Plan for European Democracy

By the year 2020, the European Commission had developed a keen understanding of the amplified effectiveness of online propaganda tools. This understanding was explicitly articulated in the Communication on the Action Plan for European Democracy.[28] The document underscored how online campaign tools have gained increased force by harnessing a combination of elements[29]:

- Personal data: The capacity to collect and utilise extensive quantities of personal data facilitates a profound comprehension of individual users. This data can include demographic information, online behaviour, preferences, and more, painting a detailed picture of each user.[30]
- Artificial intelligence: AI algorithms can scrutinise this data and discern patterns, thereby enabling the generation of highly targeted and personalised message. These algorithms can predict user behaviour and preferences with remarkable accuracy, making the messages more relevant and engaging.
- Psychological profiling: By gaining an understanding of user behaviour and preferences, AI can create messages that resonate with individual psychology. This could potentially exploit emotional vulnerabilities, making the propaganda more effective.[31]
- Complex micro-targeting techniques: These systems permit the precise delivery of customised messages to specific user segments, maximising the impact of the

[28] Communication COM/2020/790 final 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.

[29] Communication COM/2020/790 final, cit., 3.

[30] Communication COM/2020/790 final, cit., 21.

[31] Communication COM/2020/790 final, cit., 2.

propaganda. By ensuring that the right message reaches the right user at the right time, these techniques can significantly enhance the effectiveness of online propaganda campaigns.

4.2. The 2022 Strengthened Code on Disinformation and the DSA

The Strengthened Code on Disinformation of 2022 recognizes the potential for recommender systems to distort users' access to information. While it acknowledges that users can theoretically adjust settings to influence the content they see, the Code highlights the limitations of this approach. Recommender systems can be highly sophisticated, and users may not fully understand the algorithms that shape their online experience. This creates a situation where users might believe they have control over their information diet, while recommender systems can still subtly manipulate what they see.[32]

In terms of systemic risk assessment and mitigation obligations, arts. 34 and 35 of the Digital Services Act[33] mark a significant shift from self-regulation to co-regulation. These articles mandate that providers of very large online platforms (VLOPs) and search engines actively identify and address systemic risks within their services. This includes any algorithmic systems that may contribute to the spread of disinformation. Indeed, artt. 34 and 35 specifically mention «recommendation systems and advertising systems» as areas of particular scrutiny. These algorithmic systems are known to play a significant role in shaping user exposure to content, both positive and negative. The DSA compels VLOPs to assess how these systems might amplify misleading or deceptive content, even if it originates outside the platform itself. In addition, VLOPs are required to conduct regular risk assessments. This involves evaluating how their platform design, features, and algorithms contribute to the spread of disinformation. Based on this assessment, VLOPs must develop and implement mitigation strategies. These strategies could involve changes to algorithms, increased transparency around content moderation practices, or partnerships with fact-checking organizations.

The Strengthened Code on Disinformation of 2022 serves as a valuable tool within this co-regulatory framework. While not mandatory itself, the Code outlines the best practices for tackling disinformation that align with the obligations laid out in the DSA. By adhering to the Strengthened Code, VLOPs can demonstrate a proactive approach to content moderation and gain valuable insights into areas where their platforms might be susceptible to manipulation by spreaders of disinformation. This compliance with the Code can then be used as evidence towards fulfilling the legal requirements of the DSA.

In essence, the co-regulatory approach embodied by the DSA and the Strengthened Code pushes VLOPs beyond a self-regulatory model. It establishes a framework for

[32] The 2022 Strengthened Code on Disinformation, cit., 18.

[33] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

accountability and transparency in how these platforms handle the spread of disinformation.

4.3. The European Commission's Communication on defending democracy

The European Commission's recent Communication on defending democracy[34] builds upon the foundation laid by the 2020 European Democracy Action Plan. This commitment to a healthy democratic environment informs a new Recommendation focused on ensuring the integrity of European Parliament elections of 2024.[35] This Recommendation emphasizes the crucial role of political parties and political organizations in upholding fair elections. Furthermore, the Recommendation sheds light on the critical link between AI and the quality of online information available during elections.[36] Malicious use of AI systems could exacerbate the spread of disinformation and undermine public trust.

It calls for them to adopt voluntary pledges and codes of conduct that promote responsible campaigning and protect democratic values. These pledges and codes should address several key areas:

- promoting inclusive discourse: campaigns should encourage respectful debate and avoid tactics that divide or marginalize voters.
- combating manipulation: pledges should commit to avoiding tactics like spreading disinformation, using "deep fakes," or employing misleading or hateful content to influence voters. Additionally, manipulative tactics designed to amplify political messages are explicitly discouraged.
- transparency: financial contributions, including gifts and loans, along with campaign spending (especially donations exceeding set limits) must be transparent. The same goes for political advertising – its sources and content should be clearly identifiable.
- cybersecurity: campaigns should take steps like regular cybersecurity checks to protect against attacks that could disrupt elections.
- independent oversight: the Recommendation encourages independent observation of how well campaigns uphold their pledges and codes of conduct. This ensures accountability and strengthens public trust in the electoral process.

By advocating for these measures, the Commission aims to safeguard the integrity and efficiency of elections, fostering a democratic environment where citizens can make informed choices based on accurate information and respectful debate.[37]

[34] Commission Recommendation (EU) 2023/2829 of 12 December 2023 on inclusive and resilient electoral processes in the Union and enhancing the European nature and efficient conduct of the elections to the European Parliament.

[35] Commission Recommendation (EU) 2023/2829, cit., para. 1.

[36] Commission Recommendation (EU) 2023/2829, cit., para. 13.

[37] Commission Recommendation (EU) 2023/2829, cit., Whereas no. 39.

4.4. The Regulation on the transparency and targeting of political advertising

The recently adopted Regulation on the transparency and targeting of political advertising[38] recognizes the inherent tension between AI-powered user profiling and a healthy democratic information environment. By allowing political campaigns to target users with laser-like precision based on their data profiles, AI can effectively create echo chambers, limiting exposure to diverse viewpoints and potentially amplifying disinformation that resonates with pre-existing biases. The Regulation's emphasis on transparency serves as a crucial first step in addressing these concerns.[39] Indeed, when personal data is processed using targeting or ad-delivery techniques, controllers are required to adhere to certain provisions, that supplements Regulation (EU) 2016/679[40] and Regulation (EU) 2018/1725[41]. One of the key requirements is that controllers must provide additional information alongside the indication that a given piece of content is a political advertisement. This information is intended to help the individual to understand the logic and main parameters of the techniques used. It should clarify whether an artificial intelligence system has been used to target or deliver the political advertisement, and whether any additional analytical techniques have been employed. They seek to empower individuals with the knowledge and understanding of how their data is being used, who is being targeted, and why certain parameters are chosen.[42] This, in turn, can help individuals make informed decisions about their engagement with such advertisements.

[38] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising.

[39] Regulation (EU) 2024/900, cit., Whereas no. 4.

[40] 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).

[41] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

[42] Regulation (EU) 2024/900, cit., art. 19, para. 1, lit. c., according to which: «When using targeting techniques or ad-delivery techniques in the context of online political advertising involving the processing of personal data, controllers shall, in addition to other requirements laid down in this Regulation and to the requirements laid down in Regulations (EU) 2016/679 and (EU) 2018/1725, comply with the following requirements: […] provide, together with the indication that it is a political advertisement, additional information necessary to allow the individual concerned to understand the logic involved and the main parameters of the techniques used, including whether an artificial intelligence system has been used to target or deliver the political advertisement and any additional analytical techniques, and including the following elements: (i) the specific groups of recipients targeted, including the parameters used to determine the recipients to whom the advertising is disseminated; (ii) the categories of personal data used for the targeting techniques or ad-delivery techniques; (iii) the targeting goals, mechanisms and logic including the inclusion and exclusion parameters, and the reasons for choosing those parameters; (iv) meaningful information on the use of artificial intelligence systems in the targeting or ad delivery of the political advertising; (v) the period of dissemination of the political advertisement and the number of individuals to whom the political advertisement is disseminated; (vi) a link to or a clear indication of where the policy referred to in point (a) can be easily retrieved».

4.5. The European Media Freedom Act

The European Media Freedom Act[43] acknowledges a user's right to have content personalized by platforms, a process often achieved through the use of AI and algorithms. However, the EMFA expresses a significant concern: such personalization can inadvertently create echo chambers and exacerbate political polarization.

The core of the issue lies in how AI tailors content to a user's existing preferences. By analyzing past behavior and interactions, AI algorithms can predict which information a user is most likely to engage with. While this can lead to a more convenient user experience, it can also lead to a situation where users are primarily exposed to content that reinforces their existing beliefs. This "filter bubble" effect limits exposure to diverse viewpoints and potentially fuels confirmation bias, where users favor information that confirms their pre-existing biases and disregard information that contradicts them. In a healthy democracy, informed debate requires exposure to a variety of perspectives. If users only encounter information that aligns with their existing political convictions, it hinders their ability to critically evaluate different viewpoints and engage in constructive discourse. The EMFA highlights this potential danger of AI-driven personalization, emphasizing the need for safeguards that ensure users have access to a diverse range of information and are not confined to echo chambers that limit their understanding of complex issues.

4.6. The private actors

In this pivotal 'super election year', private entities were not just bystanders but active participants in safeguarding the democratic process. They took significant improvements to prevent the misuse of AI from casting a shadow over the integrity of elections. A landmark event in this regard was the Munich Security Conference held in February 2024. Here, a consortium of tech giants, including Adobe, Amazon, Google, IBM, Meta, Microsoft, OpenAI, TikTok, and X, undertook to combat the dissemination of content that could potentially undermine electoral processes.

This pact was not merely a statement of intent but included eight concrete commitments:[44]

The development and implementation of technologies to mitigate the risks associated with deceptive election content created with AI systems, including those that are open-source.

The assessment of AI models under the agreement to understand the potential dangers they may pose in relation to the production of deceptive election content.

The detection and monitoring of the distribution of such materials on their platforms.

The implementation of measures to manage deceptive information distributed on

[43] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act).

[44] For more information, visit *securityconference.org*.

their services appropriately.
The promotion of an intersectoral response to deceptive election content, fostering collaboration across different sectors.
The continued engagement with academics and civil society organizations, ensuring a multi-stakeholder approach.
The support of efforts to encourage awareness, media literacy, and societal resilience, empowering individuals to navigate the digital landscape.
An example of these efforts is the partnership between Meta and the European Commission.[45] They had joined forces to create a platform that offered users swift access to real-time content and information related to the European Parliament elections, which took place in June 2024. This platform aggregated posts on Facebook and Instagram made by candidates from each member state of the Union. It also included posts from pages and accounts that contain specific keywords, as well as institutional posts published by parties. This initiative has been a testament to the proactive steps being taken to ensure transparency and uphold the integrity of the electoral process. It underscored the crucial role of technology in fostering a healthy democratic discourse.

5. Conclusion

Election year 2024 presented unprecedented challenges to global democracy, exacerbated by the misuse of AI for the purposes of spreading disinformation and manipulating public opinion. The proliferation of fake AI-generated content highlighted the growing ability of malicious actors to undermine democratic processes. Faced with this threat, both the United States and the European Union took measures to safeguard the integrity of their elections.
The United States reconsidered its traditional non-regulatory approach in light of past election interference, considering new interpretations of the First Amendment and the potential role of the Federal Election Commission.
The European Union took a more proactive approach, as evidenced by a series of legislative and self-regulatory initiatives aimed at regulating the use of AI, promoting transparency and combating online disinformation. These measures included the strengthened Code of Conduct on Disinformation, the Digital Services Act, the European Commission Communication on the Defence of Democracy and the European Media Freedom Act.
Equally important was the proactive engagement of the private sector in countering election disinformation. Leading technology companies, including Adobe, Amazon, Google, IBM, Meta, Microsoft, OpenAI, TikTok and X, have committed to mitigating the risks posed by AI by prioritising the detection, management and transparency of misleading content. Initiatives such as the partnership between Meta and the European Commission to provide real-time information during the European Parliament elections further demonstrated these efforts.
In conclusion, protecting democratic processes in the digital age requires a multifac-

[45] *2024 European Parliamentary Elections | Live Displays*, in *help.crowdtangle.com*, June 2024.

eted approach involving governments, regulators, the private sector and civil society. The goal is not to stifle freedom of expression, but to promote a fairer and more transparent information ecosystem where citizens can exercise their right to vote based on facts, not falsehoods.

Tre osservazioni sull'*AI Act* e il suo rapporto con il diritto dei contratti

Andrea Fedi

Abstract

L'esistenza di soluzioni di IA avrà probabilmente conseguenze sul modo in cui interpretiamo e applichiamo concetti base del diritto delle obbligazioni come la prevedibilità, la colpa, la prudenza, etc. Alcuni effetti riguarderanno anche i doveri di diligenza degli amministratori di società.
Questi temi sono certamente impattati ma non pienamente regolati nell'AI Act.
Il regolamento europeo sull'IA si applicherà insieme (e non in sostituzione) al diritto civile.
È ben prevedibile che i contratti che saranno d'ora in poi negoziati conterranno clausole per integrare (quando non sovvertire) le disposizioni dell'AI Act.

The existence of AI tools will likely have consequences on the way we interpret and apply basic concepts of the law of contract, such as foreseeability, negligence, prudence, etc. That will concern the standards applicable to fiduciary duties of directors too.
The above topics are impacted but not fully regulated by the AI Act.
The EU regulation on artificial intelligence will apply in parallel with the law of contracts (and not in lieu of that).
It is reasonable to expect that parties to contracts will negotiate clauses to integrate (and in certain cases supersede) the AI Act.

Sommario

Keywords

Intelligenza artificiale – normativa di settore - diritto civile – prevedibilità – clausole contrattuali

1. Premessa

Il 2 agosto 2024 è entrato in vigore il Regolamento (UE) 2024/1689 del 13 giugno 2014, che stabilisce regole armonizzate sull'intelligenza artificiale (c.d. *AI Act*)[1].
Susseguentemente all'entrata in vigore, le previsioni dell'*AI Act* diventeranno nondimeno efficaci gradatamente, in quattro distinte e successive fasi temporali (cfr. art. 113 *AI Act*).

- La prima fase dista oramai poche settimane. Il 2 febbraio 2025, inizieranno infatti a trovare applicazione le disposizioni generali (oggetto e finalità dell'*AI Act*; ambito di applicazione oggettivo, soggettivo e territoriale; obblighi di alfabetizzazione a carico di fornitori e utilizzatori). Insieme a tali norme fondamentali, diverranno inoltre efficaci alcuni divieti[2], collegati a sistemi di AI che è radicalmente proibito immettere sul mercato, mettere in servizio o usare[3].
- Pochi mesi più tardi, il 2 agosto 2025, sarà il turno delle disposizioni sulle autorità di notifica, sugli organismi di conformità e sulle certificazioni, insieme alle norme sulle autorità di settore europee e nazionali. Nella stessa data, inizieranno anche ad avere effetto le norme sui modelli di AI per finalità generali (*general purpose* AI – GPAI) e le disposizioni sanzionatorie (disciplinate nel Capo XII dell'*AI Act*).
- L'anno seguente sarà finalmente il momento della prima applicazione di quasi tutto il resto dell'*AI Act*, ivi incluse le norme sui sistemi di AI ad alto rischio e quelle sui sistemi di AI che richiedono l'adempimento di particolari obblighi di trasparenza.
- Solo alcune norme, dedicate ai sistemi di AI ad alto rischio che sono componenti di sicurezza di prodotti soggetti a norme UE armonizzate, si applicheranno dal 2 agosto 2027, nell'ultima e quarta fase.

Una volta pienamente applicabile (e, via via che lo diviene, con riferimento alle norme

[1] Regolamento (UE) 2024/1689 del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).
Vd. Circolare Assonime 14/2024, *Il regolamento europeo sull'intelligenza artificiale: analisi ragionata della nuova disciplina e prospettive di policy per le imprese*.
Vd. anche O. Pollicino, *Regolazione e innovazione tecnologica nell' "ordinamento della rete"*.

[2] Non si deve ritenere che, tenuto conto dell'avvio dell'efficacia di questa parte dell'*AI Act* solo dal 2 febbraio 2025, le pratiche di AI contemplate dall'art. 2 fossero prima permesse. Semplicemente, quelle pratiche, fino alla fatidica data del 2 febbraio 2025, restano regolate alla luce dei rispettivi diritti nazionali degli Stati membri, in linea con i requisiti oggettivi, soggettivi, temporali e spaziali previsti da quelle norme domestiche. Così, per esempio, una pratica manipolativa o lo sfruttamento di una vulnerabilità personale per il tramite di un sistema di AI (art. 5.1.a e b *AI Act*), fino al 2 febbraio 2025, rileva in diritto italiano come dolo contrattuale, fatto illecito o, addirittura, reato: ma sempre secondo i crismi del diritto nazionale e nel suo ambito di applicabilità.

[3] I termini "immissione sul mercato" e "messa in servizio" hanno significati specifici, loro assegnati dall'art. 3.9 e 3.11 *AI Act*. Il termine "uso" non è invece definito. Anche dove i termini sono puntigliosamente definiti, non si possono escludere problemi d'interpretazione. Ad esempio, il significato di "messa a disposizione sul mercato" e "messa in servizio" è costruito attorno al concetto di "fornitura". Molto probabilmente tale concetto va tuttavia inteso non in senso restrittivo (vendita, somministrazione), ma in senso estensivo (corrispondentemente alla sua utilizzazione in altre fonti normative unionali), inclusivo di ogni forma di trasferimento e anche della prestazione di servizi e/o di licenze.

che cominceranno progressivamente a svolgere la loro efficacia), l'*AI Act* imporrà divieti, pretenderà l'osservanza di presupposti e l'adempimento di obblighi (*ex ante* ed *ex post* rispetto all'immissione sul mercato)[4], dislocherà alcuni compiti ad autorità nazionali ed europee e contemplerà sanzioni molto rilevanti per i casi d'inosservanza. È quasi inevitabile che tale imponente *corpus* normativo (180 considerando e 113 articoli) impatti, tra gli altri, il diritto civile e, segnatamente, le branche della responsabilità civile e del diritto delle obbligazioni. È con riferimento a questa seconda che si tentano qui alcune modeste e preliminari osservazioni introduttive.

2. Le conseguenze dell'AI "sul" diritto

La prima osservazione attiene all'effetto dell'AI sul diritto delle obbligazioni. A prescindere da qualsiasi regolamentazione del fenomeno, difatti, l'esistenza stessa dei sistemi di AI e la loro diffusione sul mercato (che si può assumere sarà vertiginosa sia per velocità sia per capillarità) modificheranno profondamente la realtà fattuale del mondo in cui viviamo e, per l'effetto, non potranno che influenzare il nostro sguardo sul diritto, indipendentemente e *a priori* dei tentativi di normarlo (tra cui l'*AI Act*). È invero lecito attendersi che la realtà fenomenica dell'AI in sé e per sé (cioè, in quanto esiste e a prescindere da come sia regolata) rivoluzioni il contesto nel quale attualmente agiamo e, per derivazione, scuota alcune delle tradizionali interpretazioni dello *jus positum*.

In effetti, è la prima volta che è possibile utilizzare uno strumento (l'AI), che:

- ragiona su basi diverse da quelle della logica causale (l'AI di nuova generazione inferisce i risultati sulla base di correlazioni statistiche tra i dati processati e non sulla scorta di leggi deterministiche causa-effetto)[5],
- riesce a ordinare e analizzare una messe di informazioni esponenzialmente più alta di quella che potrebbe essere gestita da qualsiasi essere umano (singolarmente o in gruppi) e
- fornisce risposte (*output*) che, in alcuni casi, proprio per le ragioni dianzi indicate, sono imprevedibili e sorprendenti, eppure corrette.

Ebbene, una delle riflessioni che si possono fare parte proprio da qui.

Le norme con le quali usualmente interagiamo sono tutte concepite su base antropocentrica o, per meglio dire, antropomorfa, perché sono pensate tenendo conto delle capacità intellettive "naturali" degli esseri umani. Così, nel codice civile ricorre il canone della "prevedibilità", che in certi contesti delimita l'ammontare dei danni contrattuali risarcibili per inadempimento colposo (art. 1225 c.c.) e, in altri ambiti, ricorre come elemento della risoluzione per eccessiva onerosità sopravvenuta (art. 1467 c.c. [6]).

[4] A carico di per fornitori, *deployer*, importatori, fornitori e rappresentanti autorizzati.

[5] I. Carnat, *Intelligenza artificiale e responsabilità civile*, in *Enciclopedia del Diritto (i Tematici)*, Responsabilità Civile, Milano, 2024, 657 ss.

[6] La risoluzione per eccessiva onerosità sopravvenuta può essere invocata solo dove derivi da avvenimenti straordinari e imprevedibili al di fuori dell'alea normale.

Sino a oggi tale prevedibilità[7] (ma anche la riconoscibilità dell'errore nel caso dell'errore-vizio; art. 1431 c.c.[8]) erano giudicate dai tribunali rispetto alle capacità "naturali" dei contraenti.

Sarà ancora possibile mantenere tale approccio in settori negoziali caratterizzati da contrattazione algoritmica *AI-based*[9] o anche solo in mercati in cui l'operatore economico professionale farà ordinariamente uso di sistemi di AI? In altri termini, laddove il contratto risulti da una negoziazione "tra macchine" come dovrà essere interpretato il sintagma normativo dell'art. 1467, per il quale bisogna tener conto della "qualità dei contraenti"? E, nei casi in cui il contratto sia comunque stipulato tra esseri umani, la vasta e normale disponibilità di sistemi di AI non dovrà forse innalzare l'asticella di ciò che è "imprevedibile" e mutare l'odierno approccio in base al quale le capacità di previsione vanno calibrate sull'uomo-medio?

Laddove strumenti di AI (o anche di GPAI) divengano diffusi quanto adesso lo sono i cellulari, non assisteremo forse inevitabilmente a una rilettura dei canoni di prevedibilità e riconoscibilità, che saranno parametrati anche alle tecnologie di AI ordinariamente e mediamente disponibili?

Invero è legittimo chiedersi se, in settori in cui l'AI dovesse trovare normale e frequente impiego, l'imprevedibilità contemplata dall'art. 1467 (o la prevedibilità di cui all'art. 1225) debba essere testata non tanto contro le capacità "umane" del contraente "naturale"[10], quanto contro le abilità "sovrumane" dei sistemi di AI diffusi in quel mercato e per quell'attività, con l'effetto di rigettare tale domanda nell'ipotesi in cui il contraente abbia mancato di "prevedere" perché non ha negligentemente adoperato il sistema di AI pur a sua disposizione o, sebbene lo abbia utilizzato, non abbia imprudentemente tenuto conto dell'oracolo artificiale.

Più alla radice, la disponibilità di sistemi di AI e l'accrescimento delle capacità intellettive oltre i limiti dell'umano, mi sembrano idonei a incidere nella carne viva dei concetti di negligenza, imperizia e imprudenza[11], nonché su quello di imputabilità di

---

[7] Con riferimento all'art. 1225, si veda Cass. civ., sez. lav., 31 luglio 2014 n. 17460, in *Diritto & Giustizia*, 2014, con nota di M. Scofferi: «La prevedibilità del danno [….] costituisce uno dei criteri di determinazione del danno risarcibile e si risolve in un giudizio astratto di probabilità del verificarsi di un futuro evento, *secondo un parametro di normale diligenza del soggetto responsabile*».
Con riferimento all'art. 1467 si veda, *ex multis*, Trib. Milano, 7 maggio 2024, in giurisprudenzadelleimprese.it: «L'eccessiva onerosità sopravvenuta della prestazione, per potere determinare, ai sensi dell'art. 1467 c.c., la risoluzione del contratto, richiede l'incidenza sul sinallagma contrattuale di eventi che non rientrano nell'ambito della normale alea contrattuale e che si caratterizzano per la loro straordinarietà, connotato di natura oggettiva che qualifica un evento in base all'apprezzamento di elementi, quali la frequenza, le dimensioni, l'intensità, suscettibili di misurazioni (e quindi, tali da consentire, attraverso analisi quantitative, classificazioni quanto meno di carattere statistico); *e per la loro imprevedibilità, che ha fondamento soggettivo, in quanto fa riferimento alla fenomenologia della conoscenza*» (corsivo dell'Autore). Così anche Cass. civ., sez. III, 19 ottobre 2006 n. 22396, in *Il civilista*, 2009, 88 con nota di B. Pezzini.

[8] Cass. civ., sez. III, 1 ottobre 1993 n. 9777, in *Giurisprudenza italiana*, 1994, I, 1536, con nota di A. Lolli. Vd. anche C. Scognamiglio, *Vizi del Consenso*, in *Enciclopedia del Diritto (i Tematici)*, Il Contratto, Milano, 2021, 1190.

[9] U. Ruffolo-A. Amidei, *Diritto dell'intelligenza artificiale*, Roma, 2024.

[10] Cass. civ., sez. II, 23 febbraio 2001 n. 2661, in *Giurisprudenza italiana*, 2001, 1824, con nota di V. Corriero.

[11] La *prevedibilità*, così come l'*evitabilità*, sono i due concetti-pilastro della colpevolezza; vd. F. Piraino, *Dolo e colpa (responsabilità civile),* in *Enciclopedia del diritto (i Tematici),* Responsabilità Civile, Milano, 2024,

un inadempimento a un soggetto[12].

Allo stesso modo, la facoltà di potersi rivolgere a sistemi superumani, che possono prevedere ciò che altrimenti è imprevedibile e suggerire condotte rimediali o per lo meno limitative del pericolo o del danno, nel settore dell'impresa potrebbe condurre a elevare la soglia di diligenza richiesta all'operatore professionale nei suoi rapporti con i consumatori, o quella richiesta agli organi di amministrazione nella gestione delle società.

Basti pensare, al riguardo, al concetto di *business judgement rule*[13] e alla ripetuta giurisprudenza che ha confermato l'assenza di responsabilità degli amministratori di società di capitali, pur nel caso di scelte *a posteriori* rivelatesi sbagliate, purché *ex ante* il processo di elaborazione della decisione (ancorché *ex post* qualificabile come errata) fosse stato corretto: raccolta scrupolosa delle informazioni, analisi delle stesse con l'ausilio di consulenti ed esperti, formazione della decisione senza azzardi.

Ebbene, di fronte alla disponibilità di sistemi di AI con enormi capacità computazionali e analitiche, sarà ancora coperto dalla *business judgement rule* l'amministratore che non abbia dotato la sua impresa di tali sistemi o non vi abbia fatto ricorso[14]?

Identicamente, tenuto conto delle enormi capacità dei sistemi di AI e della loro probabile generale diffusione, è verosimile pensare che s'innalzeranno ancora i limiti oltre i quali si potrà accedere alle esenzioni di responsabilità per "caso fortuito" o "adozione di tutte le misure idonee" (artt. 2050 e 2051 c.c., tra i tanti).

Certamente quanto sopra andrà valutato caso per caso.

I risultati interpretativi potrebbero dovrebbero infatti essere sensibilmente differenti a seconda della diffusione dei sistemi AI e della loro affidabilità e uniformità di risultati, nonché sulla base di tutte le particolarità della fattispecie, tanto in termini oggettivi,

564.

[12] La disponibilità di tecnologie AI incide evidentemente anche sul *consumer expectation test* sulla sicurezza dei prodotti, di cui alla Direttiva sulla Sicurezza dei Prodotti (direttiva 2024/2853, art. 7).

[13] M. Favaretto, *Intelligenza artificiale, sostenibilità e digitalizzazione,* in M. Callegari-E.R. Desana-R. Russo-F. Sudiero (a cura di), *Casi di diritto commerciale*, Milano, 2024, 230.

Ex multis, Cass. civ., sez. I, 25 marzo 2024, n. 8069, in *Giustizia Civile Massimario*, 2024: «In tema di responsabilità dell'amministratore per i danni cagionati alla società amministrata, il principio della insindacabilità del merito delle scelte di gestione (cd. business judgement rule), le quali possono eventualmente rilevare come giusta causa di revoca dell'amministratore, ma non come fonte di responsabilità contrattuale nei confronti della società, non si applica in presenza di *irragionevolezza, imprudenza o arbitrarietà* palese dell'iniziativa economica e, tantomeno, in caso di inequivoche violazioni di legge come, in particolare, nel caso di violazione di norme tributarie» (corsivo dell'Autore).

Spetta inoltre agli amministratori il dovere di predisporre assetti organizzativi, amministrativi e contabili *adeguati* (art. 2086 e 2381 c.c.) e, ai fini del giudizio di adeguatezza, conta evidentemente scriminare tra eventi *prevedibili* (che hanno bisogno di essere fronteggiati da assetti organizzativi già predisposti e pronti a contrastarne gli effetti negativi) ed eventi imprevedibili (vd. A. Lolli, M.G. Paolucci, *Gli assetti organizzativi adeguati e la responsabilità dell'organo amministrativo tra collegialità e organi delegati: la nuova impostazione del codice della crisi nella versione riformata dal primo "correttivo"*, in *Rivista di diritto societario*, 2, 2020, 343. Vd. anche M. De Poli, *Sulla responsabilità degli amministratori esecutivi*, in M. De Poli-G. Romagnoli (a cura di), *Le azioni di responsabilità nelle società di capitali*, Pisa, 2024, 86.

[14] A. Sacco Ginevri, *Ancora su intelligenza artificiale e corporate governance*, in *Rivista trimestrale di diritto dell'economia*, Supplemento 2, 3, 2021, 343 ss.; N. Abriani, *La corporate governance nell'era dell'algoritmo. Prolegomeni a uno studio sull'impatto dell'intelligenza artificiale sulla corporate governance*, in *Il nuovo diritto delle società*, 3, 2020, 270. M.L. Montagnani, *Flussi informativi e doveri degli amministratori di società per azioni ai tempi dell'intelligenza artificiale*, in *Persona e Mercato*, 2, 2020, 99 ss.

quanto dei soggetti che vi hanno preso parte (imprenditori, professionisti o consumatori, etc.).
Infine, non è senza importanza sottolineare che i sistemi di AI producono *output* perché rintracciano correlazioni statistiche tra dati. E, allora, non è detto che l'indicazione, da parte di un sistema di AI, di una certa regolarità statistica possa sempre automaticamente equivalere, ai fini del diritto, a un giudizio di prevedibilità.
Forse si dovrebbe invero ritenere che la prevedibilità sia intimamente collegata a una legge scientifica (in questo senso l'effetto può essere "pre"-visto, al momento in cui se ne scorge la causa che, inevitabilmente, lo produrrà); mentre potrebbe essere sottilmente differente il caso della mera ricorrenza statistica, accertata da un sistema di AI che, oltretutto, come è noto, è di per sé opaco[15].
Insomma, non troverei in linea di principio infondata una linea argomentativa che restringa la prevedibilità e la riconoscibilità a ciò che, secondo leggi causali (e non meramente statistiche), consegue a una certa circostanza. Vieppiù tenuto conto che spesso il sistema di AI presente le caratteristiche del *black box* (ossia, dal punto di vista umano, non si riesce a ricostruire il perché il sistema di AI abbia giudicato in un certo senso piuttosto che un altro).
Si tratta di temi sui quali è necessaria una riflessione molto approfondita.
Da una parte, la disponibilità di oracoli informatici animati dall'intelligenza artificiale potrebbe elevare l'asticella del *test* di diligenza in tutti quei settori dove tali sistemi di AI sono diffusi e si sono dimostrati credibili; ma, dall'altra parte, questo non può essere preso come un risultato scontato e automatico, essendoci casistiche nelle quali i sistemi di AI potrebbero essere ancora immaturi, insufficientemente addestrati, o aver fornito *output* non sempre affidabili; oppure potrebbero essere poco diffusi o estremamente costosi, o, ancora, non meritevoli di supina adesione ai loro responsi, per via della novità del settore in cui si opera e dell'opacità del loro funzionamento.

3. Il posto dell'*AI Act* "nel" diritto

La seconda questione di cui vogliamo trattare non attiene all'ambito fenomenico (e ai suoi effetti sul diritto), ma direttamente a quello giuridico ossia a quello delle norme composte in ordinamento, vertendo sulla collocazione dell'*AI Act* all'interno del diritto (civile).
La questione (gravida di conseguenze pratiche) può essere così sintetizzata:

- L'*AI Act* si muove esclusivamente sul terreno del diritto pubblico, definendo, da una parte, i compiti di controllo delle Autorità di Notifica e di Vigilanza del Mercato (art. 70 *AI Act*) e, dall'altra, i presupposti di irrogazione delle sanzioni amministrative (Capo XII *AI Act*)?
- Oppure l'*AI Act* assume valore anche dal punto di vista del diritto civile? E, in questo secondo caso, l'*AI Act* affianca e integra il diritto civile domestico degli Stati Membri UE o si sovrappone allo stesso, disciplinando in esclusiva alcune fattispe-

[15] E. Battelli, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in *Il diritto della famiglia e delle persone*, 3, 2022, 1096 ss.

cie e scalzando le norme civili nazionali?

Per semplicità e facendo un esempio: le pratiche di AI vietate (art. 5 *AI Act*) esauriscono il novero dei divieti in materia di AI anche in sede civilistica, oppure le stesse rappresentano solo l'elencazione di quelle proibizioni che le Autorità preposte devono verificare e che possono comportare una responsabilità amministrativa, impregiudicate restando però tutte le altre limitazioni e tutti gli altri divieti che possono scaturire dal codice civile, dal codice dei consumatori e dalle altre fonti *juris privatorum*?

A questa domanda possono essere date varie risposte, con varie sfumature, ma, per semplicità d'analisi, le due alternative estreme sono:

a) la tesi per cui, in ambito di sistemi di AI, le disposizioni dell'*AI Act* esauriscono la disciplina applicabile e, dunque, ciò che l'*AI Act* proibisce è vietato e tutto il resto è permesso (anche in ottica privatistica, quindi, ciò che non è vietato dall'*AI Act* è *jure* e non *contra jus*) e

b) l'antitesi per cui l'*AI Act* opera solo nel rapporto pubblicistico tra cittadino (o impresa) e Autorità, mentre, nei rapporti tra privati, operano le *rules* e gli *standards* del diritto civile domestico (*neminem laedere*, buona fede, etc.)[16].

Entrambe tali letture estreme pongono seri problemi.

- La lettura, per la quale l'*AI Act* definisce un sistema di divieti e di obblighi "esclusivo" in materia di AI (e il diritto civile domestico, comprese le sue clausole generali, è messo fuori gioco) conduce a risultati contraddittori rispetto all'architettura del diritto comunitario e paradossali rispetto alle conseguenze privatistiche.

Da un lato (quello dell'architettura delle fonti del diritto), il meccanismo articolato dal diritto unionale, che prevede separatamente un regolamento (l'*AI Act*) e una separata proposta di direttiva (per disciplinare la responsabilità extracontrattuale da AI), lascia intendere chiaramente che le questioni di responsabilità aquiliana restano nel dominio del diritto domestico, pur richiedendosi, tramite la direttiva, un allineamento dei vari diritti statuali. *Ergo*: tale meccanismo sembra chiaramente negare l'esclusiva di disciplina all'*AI Act* sulle questioni privatistiche.

Dall'altro lato (quello delle conseguenze privatistiche), portata *in extremis* l'interpretazione per cui l'*AI Act* regola in maniera uniforme ed esclusiva anche i rapporti tra privati (rimpiazzando le norme civilistiche di diritto interno) finisce per escludere l'applicabilità di una serie di norme, con risultati del tutto insoddisfacenti proprio rispetto alle finalità dell'AI Act (tra cui la tutela dei diritti fondamentali).

Consideriamo un esempio, a tal riguardo.

L'*AI Act* dispone che sono proibiti «l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative[17] o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di pren-

[16] L'*AI Act* dispone che il regolamento europeo non pregiudica alcune norme del diritto UE, ma non dice nulla sul mancato pregiudizio alle norme nazionali. Vd. Considerando 9.

[17] La capacità manipolativa rileva sia come elemento della fattispecie delle pratiche di AI vietate ai sensi dell'art. 5 dell'*AI Act*, sia come fattore di rischio sistemico per i GPAI (art. 55). Vd. *First Draft of the General-Purpose AI Code of Practice published, written by independent experts*.

dere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo» (art. 5.1.a).

Non v'è chi non veda che si tratta di una fattispecie molto simile (anche se non perfettamente coincidente) a quella del dolo-vizio del consenso ai sensi del diritto interno. Ebbene, la tesi dell'applicazione esclusiva dell'*AI Act* ci condurrebbe inevitabilmente alla conclusione, per cui un sistema di AI usato come artificio o raggiro non ricadrebbe nella disciplina domestica del dolo-vizio, ma solo in quella dei divieti di cui all'art. 5 *AI Act*.

Tale conclusione sarebbe grave.

Vero è che la violazione dell'*AI Act* (norma imperativa) comporterebbe conseguenze coerenti con l'antigiuridicità dell'evento. Sarebbe infatti plausibilmente riconosciuta la nullità, ex art. 1418 c.c., del contratto concluso a seguito dell'operare di un sistema di AI manipolativo o ingannevole e tale nullità sarebbe rilevabile *ex officio* e imprescrittibile.

Altrettanto vero è però che la sciagurata formulazione[18] dell'art. 5.1.a dell'*AI Act* sembra considerare solo il caso del dolo determinante (l'assunzione di una decisione che non sarebbe stata altrimenti presa) e non quella del dolo incidente; con il risultato che non si capirebbe più se tale dolo incidente sia rilevante ai fini giuridici (in quanto non chiaramente desumibile dalla lettera dell'AI Act). Vieppiù grave sarebbe poi osservare che l'*AI Act* sembra collegare il divieto di sistemi di AI ingannevoli alla ricorrenza di un "danno alla persona", il che, se l'*AI Act* fosse l'unica norma operativa nella fattispecie, lascerebbe sguarniti i casi di danno a una cosa, a un'*universitas*, a un azienda, a un investimento, etc..

Identici rompicapi si potrebbero poi porre con riferimento a varie altre norme. Così, per esempio, l'art. 25, commi 1.a e 2, *AI Act*, prevede che, in alcuni casi, il *deployer* che apponga il proprio nome o marchio a un sistema di AI vada considerato come unico fornitore di quel sistema di AI e che l'originario sviluppatore "non è più considerato fornitore".

Ebbene, riconoscere a tale disposizione dell'*AI Act* un effetto esclusivo, di guisa che tutte le altre norme civili non dovrebbero più trovar spazio, comporterebbe che l'originario fornitore non sia più tale neanche ai fini delle responsabilità extracontrattuali o contrattuali o consumeristiche che discendono da tale sua veste: il che è evidentemente illogico, oltre che contradditorio con altri atti di diritto dell'UE.

- Molto meglio, dunque, pensare che l'*AI Act* affianchi, ma non sostituisca, il diritto privato domestico e sia una disciplina "minima" che opera sul piano regolamentare[19], senza soppiantare le regole del diritto civile.

Tale interpretazione, tuttavia, ha bisogno di qualche distinguo.

---

[18] La norma sembra avere vari problemi di formulazione: ad esempio, l'avverbio "volutamente" che sembra riferirsi solo alle pratiche ingannevoli e manipolative e non a quelle subliminali.

[19] U. Ruffolo-A. Amidei, *Diritto dell'intelligenza artificiale*, cit. Del resto, la decisione del legislatore comunitario di consegnare il sistema della responsabilità civile a due proposte di direttiva, separate dall'*AI Act*, dimostra che la regolazione degli aspetti civili (extracontrattuali) dell'uso dell'intelligenza artificiale è intesa come materia e settore separati dal campo d'applicazione "diretto" dell'*AI Act*.

Infatti, ancorché sembri fondato affermare che l'*AI Act* non rimpiazzi il diritto civile, questo non significa che l'*AI Act* e le sue violazioni si muovano solamente sul piano pubblicistico dei rapporti tra Stato e cittadino e restino irrilevanti dal punto di vista del diritto dei contratti. Tutt'al contrario, a chi scrive pare che la mancata osservanza dell'*AI Act* possa costituire il presupposto per l'applicazione di alcune regole privatistiche.

Per esempio, la violazione, da parte del fornitore, delle norme sui sistemi di AI ad alto rischio, dovrebbe ragionevolmente innescare la sua responsabilità (anche *ex empto*[20]) per vizi o mancanza di qualità (artt. 1492 e 1497 o 1578 o 1667 c.c., a seconda dei casi di vendita, licenza sviluppo su commissione[21]).

Similmente, la commessa e la fornitura di sistemi di AI per il controllo delle emozioni dei lavoratori (art. 5.1.f *AI Act*) devono ritenersi, oltre che vietate dall'*AI Act*, anche causa di nullità del contratto per violazione di norme imperative (art. 1418 c.c.[22]).

Insomma, l'*AI Act* non rimpiazza il codice civile, ma le violazioni dell'*AI Act* sono atti o fatti illegittimi e, come tali, possono costituire elementi delle fattispecie civili considerate dal diritto domestico.

4. Gli effetti "di" diritto dell'*AI Act*

Se quanto precede è corretto, allora i contratti aventi l'AI come oggetto continueranno a essere disciplinati (anche) dalle norme del codice civile e del codice del consumo. Questo, tuttavia, apre a tutta una nuova serie di questioni di grande interesse per i cosiddetti "pratici" del diritto.

- In primo luogo, sarà d'ora in poi necessario negoziare con grande attenzione e disciplinare in modo preciso tutti i vari rapporti all'interno della *supply chain* di un sistema di AI (quelli con i programmatori, gli sviluppatori, i produttori di componenti *hardware* o

[20] Il problema gigantesco, specie nel caso dei sistemi di AI, sarà però il termine di prescrizione annuale (per la vendita) che, all'evidenza, non si concilia con la tempistica per rendersi conto dell'esistenza di un vizio del sistema.

[21] Nel caso dei programmi per elaboratore, si discute talora se la fornitura debba essere ricompresa nel *genus* vendita o in quello appalto; Cass. civ., sez. II, 9 agosto 2013, n. 19131, in *Giust. civ. Mass.* 2013: «A prescindere dalla qualificazione del contratto come vendita o appalto, l'obbligo di fornire e mettere in funzione un sistema computerizzato di software applicativo (nella specie, per la realizzazione e la gestione di una banca dati) è un'obbligazione di risultato, sicché, qualora il medesimo risultato contrattuale sia mancato, l'utente può chiedere la risoluzione del contratto».

[22] E. Navarretta, *Libertà fondamentali dell'U.E. e rapporti fra privati: il bilanciamento di interessi e i rimedi civilistici*, in F. Mezzanotte (a cura di), *Le libertà fondamentali dell'Unione Europea e il diritto privato*, Roma, 2016, 41 ss. A. Plaia, *Le patologie del contratto*, Torino, 2022, 11.

software[23], gli addestratori, i fornitori dei dati[24], etc.)[25]. Tra i temi centrali di negoziazione ci possiamo evidentemente attendere estesi *set* di dichiarazioni e garanzie, manleve[26] e obblighi di collaborazione e assistenza.

Accanto a questi aspetti, è possibile immaginare che vi saranno estese discussioni su chi debba assumere il ruolo di "fornitore" ai sensi dell'*AI Act*[27]. Alla luce della vasta messe di obblighi e responsabilità connesse a tale ruolo, non dovrebbe invero essere sorprendente un tentativo di "fuga" da tale ruolo, anche attraverso apposite clausole contrattuali. In ciò, alcune imprecisioni lessicali dell'*AI Act* potranno forse essere piegate a tale scopo.

Già la definizione di "fornitore" si presenta in effetti assai imprecisa (art. 3 *AI Act*), posto che la norma definisce il fornitore come: «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo *che sviluppa* un sistema di IA o un modello di IA per finalità generali *o che fa sviluppare* un sistema di IA o un modello di IA per finalità generali *e immette tale sistema o modello* sul mercato *o mette in servizio* il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito»[28].

Orbene, come interpretare il ricorso alla disgiuntiva "o" nel contesto di tale formulazione? Se un'impresa fa sviluppare un sistema di AI a una *software house* e quest'ultima la sviluppa e la cede alla committente, chi è il fornitore? Chi l'ha sviluppato (la *software house*) o chi lo ha fatto sviluppare (l'impresa)? O entrambi? E le responsabilità (tra chi sviluppa, chi fa sviluppare, chi immette sul mercato e chi mette in servizio) saranno solidali o parziarie?

È ben prevedibile che questi temi, non regolati dal regolamento europeo, tenteranno d'essere risolti dalle parti contrattuali, con clausole contrattuali o con un sistema di manleve o assicurazioni.

---

[23] Vd. considerando 88 e art. 25.4 *AI Act*, che prevede «Il fornitore di un sistema di IA ad alto rischio e il terzo che fornisce un sistema di IA, strumenti, servizi, componenti o processi utilizzati o integrati in un sistema di IA ad alto rischio precisano, mediante accordo scritto, le informazioni, le capacità, l'accesso tecnico e qualsiasi altra forma di assistenza necessari, sulla base dello stato dell'arte generalmente riconosciuto per permettere al fornitore del sistema di IA ad alto rischio di adempiere pienamente agli obblighi di cui al presente regolamento. Il presente paragrafo non si applica ai terzi che rendono accessibili al pubblico strumenti, servizi, processi o componenti, diversi dai modelli di IA per finalità generali, con licenza libera e open source». La norma impone la conclusione di un accordo scritto e ne elenca il contenuto minimo. Per quanto abbiamo sostenuto sopra, al paragrafo 1, con riferimento alla coesistenza dell'*AI Act* con le norme di diritto civile nazionale, la mancanza di un siffatto accordo scritto comporterà un illecito amministrativo sanzionabile, ai sensi dell'*AI Act*. Non deve però ritenersi che l'*AI Act* abbia introdotto un nuovo requisito di forma scritta *ad substantiam* o *ad probationem*; perciò, anche in assenza di atto scritto, l'analisi sull'an e sul contenuto di accordi tra il fornitore di sistemi AI e i fornitori di sue componenti continueranno a essere delibati secondo le ordinarie norme privatistiche.

[24] La qualità dei dati è l'architrave e il presupposto fondamentale per evitare allucinazioni e inquinamento da *bias*; vd. M. Bassini, *Intelligenza Artificiale generativa: alcune questioni problematiche*, in *Rivista dei media*, 2, 2023, 393.

[25] Grandi problemi di diritto internazionale privato si porranno, peraltro, laddove il contratto di fornitura sia soggetto a legge straniera, che si applicherà contemporaneamente all'*AI Act*, alle disposizioni di applicazione necessaria italiane, al GDPR, etc.

[26] Grande attenzione richiederà l'analisi di tali manleve. Non tutte saranno forzatamente valide. Dottrina e giurisprudenza sono da anni in discussione, infatti, sui limiti di validità e operatività del cd. patto di manleva. A. Franchi, *Riflessioni sulla manleva*, in *Contratto e impresa*, 1, 2017, 155.

[27] e, da un punto di vista privacy, chi sia *data controller* e chi sia *data processor*.

[28] Corsivo dell'Autore.

- In secondo luogo, il già richiamato art. 25.1.a *AI Act*[29] prevede che il *deployer,* che apponga il proprio nome o marchio a un sistema di AI, ne divenga fornitore, ma - soggiunge la norma - «fatti salvi accordi contrattuali che prevedano una diversa ripartizione degli obblighi a riguardo». Ebbene, da una parte, ci si può attendere con ragionevole certezza la negoziazione frequente di tali "accordi"; dall'altra, sarà interessante vedere quale effetto la giurisprudenza vi riconnetterà; in gioco ci sono due diverse possibili interpretazioni: la prima, per la quale l'accordo sulla "diversa ripartizione di responsabilità" ha effetto solo *inter partes* (tra fornitore e *deployer*), ma non verso i terzi; la seconda, per la quale la diversa ripartizione vale anche nei confronti dei terzi.
- Infine, nelle condizioni generali di contratto dei fornitori di sistemi AI credo sia legittimo aspettarsi una serie di clausole che, facendo leva sull'appena menzionato art. 25.1 dell'*AI Act* (ossia la norma che regola i casi in cui *deployer*, importatore, distributore assumono il ruolo di fornitore), cercheranno di interpretarne estensivamente la casistica in modo da riversare su *deployer*, importatori e distributori il peso della posizione e degli obblighi di un fornitore di servizi AI. Immagino che non sarà infrequente imbattersi, in questo senso, in condizioni generali pro-fornitore che prevedano, ad esempio, che qualsiasi modifica del sistema di AI debba intendersi sostanziale[30], o qualsiasi uso di un nome (anche se non del marchio) inneschi la trasmissione del ruolo di fornitore, o, ancora, qualsiasi mutamento di finalità del sistema di AI faccia scattare l'acquisizione del ruolo di fornitore.

Non sembra neppure possibile escludere la negoziazione di dichiarazioni e garanzie per così dire "inverse" (ossia rese dal cliente al fornitore) - ad es., che l'acquirente del sistema di AI ha un alto livello di alfabetizzazione, ha struttura e organizzazione perfettamente idonea non solo a rispettare gli obblighi dell'*AI Act* ma a evitare ogni rischio, che ha pienamente compreso le istruzioni d'uso e le accetta come totalmente soddisfacenti, etc.

Tutte queste clausole saranno verosimilmente chieste dai fornitori per escludere le proprie responsabilità o, quanto meno, per ridurle *ex* art. 1227 c.c.

Eppure, queste stesse clausole in qualche modo rovesceranno l'assetto di obblighi e responsabilità pensato dall'*AI Act*. Resisteranno queste clausole a tale censura?

Ci aspettano tempi interessanti.

[29] Vd. anche considerando 84 *AI Act*.

[30] *Quid*, ad esempio, nel caso di customizzazione di un sistema di AI?

Dark pattern e personalizzazione manipolativa: *fit check* del panorama legislativo europeo*

Edoardo Gatelli

Abstract

I *dark pattern* sono tecniche di manipolazione degli utenti in ambito digitale il cui impiego si colloca in una zona grigia tra legittimi tentativi di persuasione a fini commerciali e influenze indebite nel processo decisionale dei consumatori. Negli ultimi anni, il progresso tecnologico in ambiti quali la raccolta dati, la profilazione e l'intelligenza artificiale, ha portato le più recenti forme di manipolazione degli utenti ad un livello di persuasione molto più allarmante rispetto a quelli che ormai è possibile considerare come *dark pattern* tradizionali. Il quadro normativo europeo, se paragonato alla risposta pressoché soddisfacente del legislatore alle sfide poste dalla prima generazione di *dark pattern*, non appare altrettanto al passo coi tempi in relazione a questa nuova frontiera della manipolazione digitale; il principale punto di riferimento resta, infatti, il Regolamento generale sulla protezione dei dati (GDPR).

The employment of dark patterns – *i.e.* digital deceptive techniques aimed at manipulating users in the digital environment – falls in a blurred area between legitimate persuasion attempts for commercial purposes and undue influences in the decision-making process of consumers. In recent years, the technological advancement in such fields as data collection, profiling and artificial intelligence have brought the latest forms of user manipulation to another level with respect to what can by now be considered as traditional dark patterns. The European regulatory framework, if compared to the regulatory response to the challenges posed by first generation dark patterns, appears outdated towards this new frontier of digital manipulation and, therefore, the key to assess these phenomena from a legal perspective remains within the General Data Protection Regulation (GDPR).

*Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

Edoardo Gatelli

Sommario

Keywords

dark pattern, manipolazione, personalizzazione, profilazione, GDPR.

1. Definizioni

I *dark pattern* possono essere definiti tecniche ingannevoli basate su tecnologie informatiche, più o meno complesse, strumentali alla manipolazione dei consumatori in ambito digitale. L'impiego di queste tecniche si colloca in una zona grigia tra legittimi tentativi di persuasione a fini commerciali e influenze indebite nel processo decisionale degli utenti. Il termine *dark pattern* venne coniato nel 2010 da Harry Brignull sul sito "*darkpatterns.org*"[1] in un pionieristico tentativo di catalogare le pratiche sleali rilevate con maggiore frequenza sulle piattaforme digitali di uso comune. L'espressione deriva dalla nozione di *design pattern* in ingegneria del software, ossia una soluzione generale e ripetibile ad un problema ricorrente nella progettazione software[2]. Pertanto, se l'idea di design pattern è quella di indentificare un problema e la relativa soluzione, astrarla dal caso specifico e modellarla in maniera più generica per poterla riutilizzare applicandola in diversi scenari, i *dark pattern* possono essere considerati come una particolare tipologia di *design pattern* intrinsecamente maligna e specificamente concepita per ingannare e manipolare gli utenti. Ad oggi, rinunciando al *pathos* del vocabolo "*dark*" in favore del più evocativo e chiaro "*deceptive*", il neologismo si è evoluto in "*deceptive patterns*", per quanto i due termini possano comunque essere utilizzati come sinonimi. Nel 2022, la Direzione generale della Giustizia e dei consumatori della Commissione europea ha pubblicato un report che fornisce una definizione generale del fenomeno, enucleando sommariamente le diverse caratteristiche catalogate dalla letteratura esistente sui *dark pattern*. In particolare, il report propone la seguente nozione di *dark pattern*: «*practices in digital interfaces that steer, deceive, coerce, or manipulate consumers into making choices that often are not in their best interests*»[3]. Rientrano in questa definizione, dunque, tutte le tecniche implementate in ambito digitale finalizzate a indurre, ingannare, costringere o manipolare gli utenti a prendere decisioni che, nella maggior parte dei casi, si rivelano contro il loro stesso interesse. Tuttavia, il report sottolinea anche l'esigenza di superare le singole definizioni specifiche, poiché, dal punto di vista del diritto dei consumatori dell'UE, esiste un concetto generale capace di comprendere tutte le pra-

[1] Vedi H. Brignull, *Dark Patterns: Deception vs. Honesty in UI Design*, in *A list apart: interaction design, usability,* 338, 1 novembre 2011.

[2] Vedi E. Gamma-J. Vlissides-R. Helm-R. Johnson, *Design Patterns: Elements of Reusable Object-Oriented Software*, in *Addison-Wesley Professional*, 31 ottobre 1994, 2.

[3] F. Lupiáñez-Villanueva-A. Boluda-F. Bogliacino-G. Liva-L. Lechardoy-T. Rodríguez De Las Heras Ballell, *Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report*, in *Publications Office of the European Union*, aprile 2022, 20.

tiche commerciali manipolative a danno dei consumatori, indipendentemente dalle modalità utilizzate, ossia 'pratica commerciale sleale' ai sensi della direttiva 2005/29/CE[4] ("UCPD").

2. I *dark pattern* "tradizionali" e la tutela dei consumatori

È infatti possibile considerare la quasi totalità dei *dark pattern* catalogati dalla letteratura esistente[5] come pratiche commerciali scorrette alla luce della direttiva sulle pratiche commerciali sleali e, nonostante la sua entrata in vigore risalga a quasi vent'anni fa, l'UCPD grazie alla sua versatilità ancora oggi rappresenta la principale risposta del legislatore europeo alle pratiche commerciali scorrette in ambito digitale. Il che è stato reso possibile anche dalla ventata d'aria fresca portata dalla direttiva 2019/2161/UE (Direttiva *Omnibus*)[6] che ha esteso la normativa vigente adattandola a contenuti e servizi digitali, introducendo nell'UCPD disposizioni inedite come la disciplina dei motori di ricerca e delle recensioni online, rinforzando gli obblighi di informazione, introducendo la nozione di *ranking* e includendo servizi e contenuti digitali nella definizione di prodotto. Di contro, il regolamento 2022/2065/UE[7], c.d. *Digital Services Act* (DSA), non risulta applicabile ai *dark pattern*, nonostante il suo obiettivo fosse proprio quello di rivedere il quadro legislativo delineato dalla Direttiva sul commercio elettronico al fine di modernizzare l'approccio del legislatore europeo nell'affrontare le nuove sfide poste dai servizi online. Infatti, è possibile relegare il campo di applicazione del DSA alle pratiche commerciali sleali tra imprese (B2B), quantomeno per il momento. In particolare, nonostante il primo comma dell'articolo 25 del DSA introduca il primo divieto esplicito ai *dark pattern*, il secondo comma della medesima disposizione ne esclude l'applicabilità a quelle pratiche già disciplinate dal GDPR o dall'UCPD, ridimensionandone notevolmente la portata applicativa.

[4] Direttiva 2005/29/CE del Parlamento europeo e del Consiglio dell'11 maggio 2005 relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio (Direttiva sulle pratiche commerciali sleali o Unfair Commercial Practices Directive).

[5] Secondo la tassonomia proposta nel report pubblicato dalla commissione europea, le uniche due tipologie di *dark pattern* identificate che non risultano a tutti gli effetti riconducibili alle previsioni della direttiva 2005/29/CE sono i cd. *infinite scroll* e *autoplay*, vedi ivi, 67.

[6] Direttiva (UE) 2019/2161 del Parlamento europeo e del Consiglio del 27 novembre 2019 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori.

[7] 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 o *Digital Services Act*).

3. Le nuove frontiere della personalizzazione manipolativa

Tuttavia, è fondamentale operare una distinzione tra i *dark pattern* "tradizionali", ossia quelli al centro dalla letteratura del primo decennio di tentativi di inquadramento del fenomeno in categorizzazioni sistematiche[8], e i *dark pattern* di seconda generazione. Infatti, negli ultimi anni, grazie al progresso tecnologico in ambiti come la raccolta dati, la profilazione e l'intelligenza artificiale, la progenie delle tattiche di manipolazione degli utenti nell'ecosistema digitale è diventata di gran lunga più subdola e allarmante rispetto a quelli che ormai è possibile considerare come *dark pattern* tradizionali. In particolare, di pari passo alla crescita esponenziale e disponibilità senza precedenti di vasti insiemi di dati (*big data*), le tecniche di raccolta dati, profilazione e targhettizzazione vengono sempre più implementate nel marketing digitale e abbinate alle sofisticate tecnologie di sviluppo degli algoritmi che governano le piattaforme digitali, fornendo terreno fertile per la proliferazione delle tecniche di manipolazione degli utenti incentrate sulla personalizzazione 'guidata dai dati' (*data-driven*). La genesi dei *dark pattern* di seconda generazione risiede proprio nell'integrazione di queste tecniche ai dark pattern tradizionali, aumentandone considerevolmente l'efficacia grazie alla possibilità di modellare la manipolazione alle specifiche caratteristiche di determinati gruppi di utenti, personalizzando dunque la manipolazione. Con riguardo a questa nuova forma di *deceptive pattern*, la risposta del legislatore europeo risulta anacronistica se paragonata agli avanzamenti tecnologici in questi campi, ma l'*Artificial Intelligence Act* e l'*Artificial Intelligence Liability Directive* promettono di riportare il quadro normativo comunitario al passo coi tempi. Tuttavia, un'analisi dell'impatto di questi nuovi interventi sull'impianto normativo europeo risulterebbe precoce – non essendo ancora applicabili – e, per questa ragione, l'attuale punto di riferimento nel panorama legislativo comunitario resta dunque il Regolamento generale sulla protezione dei dati[9] (GDPR).

4. Il GDPR e i *dark pattern* di seconda generazione

Al sesto considerando, il regolamento (UE) 2016/679 esordisce sottolineando la ne-

[8] Vedi G. Conti-E. Sobiesk, *Malicious interface design: exploiting the user*, in *Proceedings of the 19th international conference on World wide web (WWW '10),* 2010, 272; vedi anche C. Bösch-B. Erb-F. Kargl-H. Kopp-S. Pfattheicher, *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*, in *Proceedings on Privacy Enhancing Technologies*, 2016; vedi anche C. M. Gray-Y. Kou-B. Battles-J. Hoggatt-A. L. Toombs, *The Dark (Patterns) Side of UX Design* in, *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18), 2018; vedi anche A. Mathur-G. Acar-M. J. Friedman-E. Lucherini-J. Mayer-M. Chetty-A. Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites* in *Proc. ACM Hum.-Comput. Interact. 3, CSCW, Article 81*, 7 novembre 2019; vedi anche M. Leiser, *Illuminating Manipulative Design: from 'Dark Patterns' to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive*, in *Loyola Consumer Law Review,* 14 aprile 2022.

[9] 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 (Regolamento generale sulla protezione dei dati o *General Data Protection Regulation*).

cessità di far fronte alle dinamiche di mercato in costante evoluzione:

> «La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano»[10].

Il principale riferimento alla personalizzazione *data-driven* all'interno del GDPR è rinvenibile all'articolo 22, rubricato «Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione»[11]. La norma garantisce all'interessato (ossia la persona fisica alla quale il dato personale si riferisce)[12] «il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona»[13]. Tuttavia, il seguente punto della medesima disposizione elenca le seguenti eccezioni, al ricorrere delle quali il primo comma non trova applicazione:

- «sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento»[14];
- «sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato»[15];
- «si basi sul consenso esplicito dell'interessato»[16].

Inoltre, è rilevante sottolineare come al terzo comma la norma impone al titolare del trattamento[17] l'obbligo, nell'eventualità in cui la decisione sia necessaria per la conclusione o l'esecuzione di un contratto tra le parti o si basi sul consenso esplicito dell'interessato, di adottare «misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione»[18]. Essenzialmente, salvo le suddette eccezioni, al fine di accertare la riconducibilità di una determinata tecnica di personalizzazione alla fattispecie delineata dal primo comma dell'articolo 22 del GDPR, è fondamentale stabilire se la decisione sia stata presa

[10] Considerando 6, GDPR.

[11] Art. 22, GDPR.

[12] Vedi art. 4, n. 1, GDPR.

[13] Art. 22, par. 1, GDPR.

[14] Art. 22, par. 2, lett. a), GDPR.

[15] Ivi, lett. b).

[16] Ivi, lett. c)

[17] Vedi art. 4, n. 7), GDPR.

[18] Art. 22, par. 3, GDPR.

esclusivamente sulla base di un trattamento automatizzato dei dati e se la stessa sia tale da produrre un effetto giuridicamente rilevante per l'interessato o qualsiasi altra conseguenza ad esso paragonabile sulla sua persona. Il testo del GDPR non contiene però alcuna specifica menzione alla personalizzazione manipolativa e pertanto è alle nozioni di profilazione e di processo decisionale automatizzato che bisogna fare riferimento. Il regolamento definisce la profilazione come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica»[19]. Alla luce di questa nozione è quindi possibile evidenziare alcuni aspetti caratterizzanti della profilazione: il trattamento dei dati dev'essere automatizzato, deve riguardare dati personali e tale trattamento dev'essere strumentale alla valutazione di certi aspetti personali dell'interessato. Per quanto concerne invece il processo decisionale automatizzato, il GDPR si limita a menzionarlo senza fornirne una specifica definizione, la quale dev'essere ricavata invece dalle "Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679"[20]: «*the ability to make decisions by technological means without human involvement*»[21], ossia la capacità di elaborare una decisione tramite strumenti tecnologici senza il coinvolgimento dell'essere umano. Le Linee guida precisano poi come – per quanto il trattamento dei dati relativo ad un processo decisionale automatizzato possa portare alla profilazione – i processi decisionali automatizzati prescindono dalla profilazione, e viceversa, sottolineando dunque come le due tecniche non siano in rapporto di interdipendenza. Infine, le Linee guida includono anche il seguente catalogo dei riferimenti normativi di profilazione e processo decisionale automatizzato nel testo del GDPR, il che risulta particolarmente utile nel sintetizzare efficacemente in una panoramica il modo in cui il regolamento disciplina la personalizzazione guidata dai dati.

«Principali disposizioni del Regolamento che fanno riferimento alla profilazione e al processo decisionale automatizzato in generale»[22]

[19] Art. 4, n. 4, GDPR.

[20] Gruppo di Lavoro Articolo 29 per la Protezione dei Dati, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 3 ottobre 2017, disponibile su ec.europa.eu

[21] Ivi, 8.

[22] Gruppo di Lavoro Articolo 29 per la Protezione dei Dati, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, allegato 2, 37, 3 ottobre 2017, disponibile su ec.europa.eu

Articolo	Considerando	Osservazioni
3, paragrafo 2, lettera b)	**24**	Il monitoraggio del comportamento [degli interessati] nella misura in cui tale comportamento ha luogo all'interno dell'Unione. **Considerando 24:** " (...) tracciate su internet (...) ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, *in particolare per adottare decisioni* che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali".
4, paragrafo 4	**30**	**Articolo 4, paragrafo 4** definizione di profilazione **Considerando 30:** "identificativi online (...), quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza (...) possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, *possono essere utilizzate per creare profili delle persone fisiche e identificarle*".
5 e 6	**72**	**Considerando 72**: "la profilazione è soggetta alle norme del presente regolamento che disciplinano il trattamento dei dati personali, quali le basi giuridiche del trattamento **(articolo 6)** o i principi di protezione dei dati **(articolo 5)**".
8	**38**	Utilizzo dei dati personali dei minori per la profilazione. **Considerando 38:** "I minori meritano una specifica protezione (...) in particolare [in merito al]l'utilizzo dei dati personali dei minori a fini di (...) creazione di profili di personalità o di utente".
13 e 14	**60**	Diritto di essere informato. **Considerando 60**: "inoltre l'interessato [*deve] essere informato dell'esistenza di una profilazione e delle conseguenze della stessa*".
15	**63**	Diritto di accesso. **Considerando 63:** "diritto di conoscere e ottenere comunicazioni (...) in relazione alla finalità per cui i dati personali sono trattati (...) e, *almeno* quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento".
21, paragrafi 1, 2 e 3	**70**	Diritto di opposizione alla profilazione. **Considerando 70:** "(…) il diritto (...) di opporsi a tale trattamento (...), compresa la profilazione nella misura in cui sia connessa a tale marketing diretto".
23	**73**	**Considerando 73:** "il diritto dell'Unione o degli Stati membri può imporre limitazioni a specifici principi e (...) al diritto di opporsi, alle decisioni basate sulla profilazione (...), ove ciò sia necessario e proporzionato in una società democratica (...)" per la tutela di obiettivi specifici di interesse pubblico generale.
35, paragrafo 3, lettera a)	**91**	Una valutazione d'impatto sulla protezione dei dati è necessaria nel caso di una "valutazione sistematica e globale di aspetti personali relativi a persone fisiche, *basata* su un trattamento automatizzato, che include la profilazione, e in base al quale si adottano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche". **Riguarda il processo decisionale, compresa la profilazione, che è non si basa unicamente su un trattamento automatizzato.**

5. I principi generali del GDPR

Risulta dunque lecito affermare che la personalizzazione *data-driven* non è universalmente proibita quanto, piuttosto, subordinata al rispetto delle previsioni del GDPR o più in generale della normativa vigente. A tal riguardo, è essenziale quantomeno accennare i punti cardine del regolamento ai quali è possibile ricondurre la maggior parte delle tecniche di manipolazione online. Il principio generale è quello della correttezza del trattamento dei dati personali sancito al primo comma dell'articolo 5 del GDPR, che impone un «trattamento dei dati lecito, corretto e trasparente nei confronti dell'interessato»[23]. Questo principio generale esige tuttavia di essere articolato lungo i tre pilastri del GDPR: la trasparenza, la limitazione dello scopo del trattamento e la minimizzazione dei dati. Innanzitutto, il principio di trasparenza emerge dal combinato disposto del principio di correttezza con il primo comma dell'articolo 12 del GDPR, che impone ai titolari del trattamento l'adozione di «misure appropriate per fornire all'interessato tutte le informazioni […] e le comunicazioni […] relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro». Sulla base di tale principio, nel 2022 l'Autorità garante per la protezione dei dati francese (CNIL) ha comminato una sanzione di 150 milioni di euro a Google per non aver fornito informazioni facilmente accessibili dagli utenti sul trattamento dei loro dati personali[24]. Per quanto concerne invece il principio di limitazione dello scopo del trattamento, la lettera B del primo comma dell'articolo 5 del GDPR sancisce come i dati personali debbano essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità»[25]. Il terzo principio fondamentale da considerare nell'analisi del GDPR in relazione al fenomeno dei *dark pattern* è poi sancito dalla lettera C del primo comma dell'articolo 5 del GDPR, la c.d. minimizzazione dei dati, che impone che i dati personali siano «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati»[26]. È rilevante, tuttavia, menzionare un ulteriore concetto fondamentale per l'applicazione del GDPR, ossia quello del consenso dell'interessato, in quanto molte delle tattiche di manipolazione degli utenti in esame sono finalizzate ad indurre gli utenti a prestare il proprio consenso al trattamento dei dati senza che sussistano quei requisiti di «volontà libera, specifica, informata e inequivocabile dell'interessato»[27] che dovrebbero invece caratterizzare l'espressione del consenso secondo il GDPR.

Infine, è fondamentale anche il riferimento alle Linee guida pubblicate nel 2022 dal Comitato europeo per la protezione dei dati (EDPB) in merito all'implementazione di *deceptive pattern* nelle piattaforme di social media[28], che predispongono una classificazio-

[23] Art. 5, par. 1, lett. a), GDPR.

[24] Vedi Commission Nationale de l'Informatique et des libertés [CNIL], *Deliberation of the restricted committee No. SAN-2021-023 of 31 December 2021 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED*, 31 dicembre 2021, disponibile su *cnil.fr*

[25] Art. 5, par. 1, lett. b), GDPR.

[26] Art. 5, par. 1, lett. c), GDPR.

[27] Art. 4, n. 11, GDPR.

[28] Comitato europeo per la protezione dei dati, *Guidelines 03/2022 on Deceptive design patterns in social media*

ne delle diverse tecniche riconducendole alla rispettiva previsione del GDPR potenzialmente violata. In aggiunta, le Linee guida hanno proposto anche la distinzione tra «*content-based patterns*»[29], cioè tecniche basate sul contenuto effettivo delle informazioni veicolate agli utenti, sul modo in cui vengono formulate e il contesto nel quale vengono fornite, e gli «*interface-based patterns*»[30], ossia quelle tattiche che sfruttano le modalità di visualizzazione dei contenuti e di interazione con gli stessi da parte degli utenti.

platform interfaces: how to recognise and avoid them. Version 2.0, 14 February 2023, disponible su edpb.europa.eu

[29] Ivi, 10.

[30] *Ibid.*

Elenco autori

Maria Romana Allegri
professoressa associata di Istituzioni di diritto pubblico, Sapienza Università di Roma

Jacopo Antonelli Dudan
avvocato in Milano

Maria Esmeralda Bucalo
professoressa associata di Diritto costituzionale e pubblico, Università degli Studi di Palermo

Alfonso Contaldo
docente a contratto di Diritto dei dati, Università di Roma Tre

Elena Falletti
professoressa associata di Diritto privato comparato, Università Carlo Cattaneo-LIUC di Castellanza

Andrea Fedi
avvocato in Roma

Alessia Forte
dottoranda di ricerca in Diritto costituzionale, Università degli Studi di Milano

Chiara Gallese
Marie Sklodowska Curie postdoctoral fellow, Università di Torino

Edoardo Gatelli
dottore in Giurisprudenza

Antonio Manganelli
adjunct professor of Competition Law and Policy, Università degli Studi di Siena

Sara Mastrapasqua
dottoranda di ricerca in Diritto processuale penale, Università degli Studi di Milano

Giuseppe Muto
dottorando di ricerca in Diritto costituzionale, Università Bocconi

Alessandro Nascimbeni
dottorando di ricerca in Diritto processuale penale, Università degli Studi di Milano-Bicocca

Giovanni Negri
giornalista de Il Sole 24 ore

Stella Romano
avvocato in Verona; professoressa a contratto, Università di Bologna

Marianna Russo
ricercatrice in Diritto del lavoro, Università degli Studi della Campania Luigi Vanvitelli

Giorgio Sichera
dottore di ricerca in Diritti e Istituzioni, Università di Torino

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 2024 - CODICE ISSN 2532-9146