Ordine internazionale e diritti umani
International Legal Order and Human Rights
Ordenamiento Jurídico Internacional y Derechos Humanos
Ordre Juridique International et Droits de l'Homme
Diretta da Claudio Zanghì, Lina Panella, Carlo Curti Gialdino
EDITORIALE SCIENTIFICA

CRISTINA GRIECO*

DAL *MICROTARGETING* POLITICO AI *DEEPFAKE*: COME LE NUOVE TECNOLOGIE STANNO RISCRIVENDO LA DEMOCRAZIA IN EUROPA

1. *Introduzione*

L'impiego sempre più ampio e pervasivo delle nuove tecnologie[1] sta sollevando interrogativi inediti capaci di mettere in discussione la tenuta dei sistemi democratici[2]. L'utilizzo di algoritmi di profilazione e di sofisticati strumenti di *microtargeting* nella comunicazione politica, la diffusione di contenuti manipolati, i *deepfake* e la creazione di *filter bubble* nei *social media* sono in grado di incidere sull'opinione collettiva e di amplificare fenomeni di polarizzazione del dibattito pubblico e di disinformazione[3].

In un simile contesto, nel consueto bilanciamento dei tradizionali poteri statali – legislativo, esecutivo e giudiziario – all'interno del quale va altresì considerato il ruolo dell'informazione, ormai comunemente considerata alla stregua di un quarto potere, si è imposto un ulteriore polo di influenza, quello computazionale[4], rappresentato dalle tecnologie digitali e dai grandi attori del settore. In effetti, per l'entità dell'influenza che le

* Ricercatore in *Tenure Track* in Diritto dell'Unione europea, Università degli Studi di Macerata, Dipartimento di Giurisprudenza, Dipartimento di Eccellenza 2023-2027.

[1] L. FLORIDI, *The Fourth Revolution. How the Infosphere is Reshaping Human Reality*, Oxford, 2014.

[2] O. POLLICINO, P. DUNN, *Intelligenza artificiale e democrazia. Opportuità e rischi di disinformazione e discriminazione*, Milano, 2022, p. 1 ss.

[3] La disinformazione è la diffusione intenzionale di informazioni false o fuorvianti per influenzare il dibattito pubblico o i processi elettorali, anche tramite contenuti formalmente leciti. Si distingue dalla misinformazione, che invece è la condivisione involontaria di notizie errate. Si veda la definizione proposta dalla Commissione europea all'interno della Comunicazione COM/2020/790 final del 3 dicembre 2020, sul *Piano d'azione per la democrazia europea*, p. 20. Si veda altresì European Commission, *A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation*, Luxembourg, 2018, p. 10.

[4] Sul punto M. DURANTE, *Potere computazionale: l'impatto delle ICT su diritto, società, sapere*, Milano, 2019.

Tech Giants sono in grado di esercitare risultano sempre più assimilabili a poteri parastatali, delle vere e proprie oligarchie del digitale, in grado di condizionare in modo significativo anche il dibattito politico. Per comprendere la portata del fenomeno, basti considerare che la capitalizzazione di mercato delle sole *Google, Microsoft, Apple, Meta, Alphabet* e *Tesla* sfiora la metà del PIL statunitense e si avvicina all'intero PIL dell'Unione europea.

La fiducia nella *governance* digitale appare dunque strettamente correlata alla capacità del legislatore sovranazionale di assicurare che sul mercato vengano immessi sistemi e servizi affidabili, verificabili, conformi a elevati *standard* di sicurezza[5] all'interno dei quali venga promosso un approccio *digital by default, inclusive by design*.

In una simile prospettiva, il processo di integrazione europea appare sempre più legato ad una dimensione nuova, quella della coesione digitale, che viene ad affiancarsi ai tradizionali ambiti economico, sociale e territoriale.

Alla luce di quanto sopra, il presente contributo si propone di analizzare l'attuale quadro giuridico europeo al fine di valutarne l'idoneità a salvaguardare la democrazia e i cittadini da fenomeni come la disinformazione, il *microtargeting* politico e la manipolazione *online*.

2. *I rischi del* microtargeting *politico e di un* gerrymandering *digitale: l'azione europea a difesa della democrazia*

Nell'attuale contesto del cosiddetto "capitalismo della sorveglianza"[6], il crescente impiego delle tecnologie digitali e dei *social media* per finalità manipolative suscita rilevanti preoccupazioni sotto il profilo della tutela delle libertà individuali e di stampa. L'utilizzo non neutrale di tali strumenti rischia, infatti, di compromettere la fiducia dei cittadini nelle istituzioni democratiche, con potenziali ricadute sull'integrità del dibattito pubblico.

L'anno 2024, caratterizzato da un numero eccezionalmente elevato di tornate elettorali, ha rappresentato un punto di svolta negli equilibri geopolitici globali[7]. In un simile scenario, si è delineato con chiarezza il ruolo ormai imprescindibile dei *social media* quali strumenti di propaganda e mobilitazione elettorale, parallelamente all'emersione di nuovi e gravi rischi connessi alla diffusione di disinformazione, alla produzione di *deepfake* e alle interferenze di soggetti esterni. Tali fenomeni sono stati qualificati come una vera e propria "minaccia ibrida" per la democrazia, idonea a compromettere sia l'integrità delle consultazioni elettorali, sia il corretto funzionamento delle istituzioni rappresentative[8].

---

[5] Sul tema nuove tecnologie e diritti fondamentali si vedano P. DE PASQUALE, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?*, in *Il Diritto dell'Unione europea – Osservatorio*, 17 marzo 2022; A. ADINOLFI, *Evoluzione tecnologica e diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, in *I Post di AISDUE*, 2023, p. 323 ss.; C. GRIECO, *Intelligenza artificiale e tutela degli utenti nel diritto dell'Unione europea*, Napoli, 2023.

[6] S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London, 2019.

[7] O. POLLICINO, P. DUNN, *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi (ed opportunità)*, in *federalismi.it*, 29 maggio 2024, p. 12; G. M. RUOTOLO, *Nell'anno delle elezioni hanno tutti ragione. Alcune considerazioni sul ruolo di Diritto internazionale ed UE nel contrasto alla disinformazione*, in *SIDIblog*, 5 aprile 2024.

[8] Nella comunicazione della Commissione C/2024/3014 del 26 aprile 2024, *Orientamenti della Commissione per i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi sull'attenuazione dei rischi sistemici per i processi elettorali a norma dell'articolo 35, paragrafo 3, del regolamento (UE) 2022/2065*, al par. 63

Sono emblematici, a livello internazionale, alcuni casi in cui è emerso con forza il tema dell'uso strategico e offensivo della disinformazione come strumento politico e antidemocratico, al punto da introdurre nel dibattito pubblico l'espressione di *first social media war*[9]. Tra gli episodi più significativi si segnalano il caso *Pizzagate* e la teoria cospirativa *QAnon*[10], le dinamiche legate alla piattaforma *X* e il ruolo assunto da Elon Musk nelle recenti consultazioni elettorali statunitensi[11], il caso mediatico di *Lisa F.*[12], nonché il noto scandalo internazionale che ha coinvolto *Cambridge Analytica*[13].

Tali vicende esemplificano la portata eversiva e destabilizzante della disinformazione digitale rispetto alla tutela della democrazia e all'integrità dei processi elettorali. La sistematica diffusione di *deepfake*, specie quando orchestrata da attori statali esteri, determina un grave inquinamento del dibattito pubblico e compromette il pieno esercizio della libertà di espressione e del diritto all'informazione, essenziale per il corretto funzionamento di ogni ordinamento democratico[14]. Ne è un esempio la recente decisione della Corte costituzionale rumena[15] di annullare le elezioni presidenziali per sospette interferenze russe legate a una campagna elettorale condotta dal candidato Georgescu, prevalentemente *online* e, precisamente, su *TikTok*[16].

---

nel concetto di minaccia ibrida, vengono inclusi la disinformazione, la manipolazione delle informazioni, le ingerenze da parte di attori stranieri, ma anche gli attacchi informatici.

[9] P. SUCIU, *Is Russia's Invasion of Ukraine the First Social Media War*, in *Forbes*, March 2022.

[10] Nel 2016, il caso *Pizzagate* nacque da interpretazioni distorte di email pubblicate da WikiLeaks, trasformate *online* in una falsa accusa secondo cui una pizzeria di Washington sarebbe stata la sede di un traffico di minori coinvolgente figure politiche democratiche; la teoria portò persino un uomo armato a irrompere nel locale senza trovare nulla. La teoria *QAnon* dal 2017 ampliò questo filone, sostenendo che un'élite globale di pedofili e satanisti controllerebbe la politica e i media, mentre un presunto informatore chiamato "Q" rivelerebbe *online* indizi criptici su un imminente "grande risveglio"; nessuna prova ha mai confermato tali affermazioni, ma il movimento ha influenzato gruppi estremisti e dinamiche politiche reali.

[11] Elon Musk ha assunto un ruolo attivo nelle recenti elezioni statunitensi, sostenendo politicamente Donald Trump e usando la piattaforma X per influenzare il dibattito pubblico. Ha finanziato un super-PAC che ha promosso iniziative pro-Trump e campagne mediatiche ad alto impatto. Ha promosso un'iniziativa definita 'lotteria', che offriva fino a un milione di dollari al giorno agli elettori registrati negli *swing States*, presentandola come un progetto civico di partecipazione democratica. Le autorità hanno però segnalato possibili violazioni della legge sul voto, interpretandola come un incentivo illegale agli elettori.

[12] Nel 2016, il caso di *Lisa F.* in Germania ha riguardato una ragazza russo-tedesca che denunciò un rapimento e stupro da parte di migranti. L'indagine dimostrò che la storia era inventata, ma la notizia iniziale generò scalpore mediatico, proteste e tensioni diplomatiche tra Germania e Russia.

[13] Il noto scandalo *Cambridge Analytica* esplose nel 2018 quando emerse che la società aveva raccolto impropriamente i dati di milioni di utenti Facebook tramite un'app di quiz e che questi dati furono poi rinvenduti e utilizzati per creare profili psicologici e influenzare campagne politiche, tra cui Brexit e le elezioni USA 2016.

[14] Nella celebre sentenza *Handyside c. Regno Unito*, ric. 5493/72, sentenza del 7 dicembre 1976, para. 49, la Corte EDU ha posto in luce la duplice valenza della libertà di espressione, quale presupposto essenziale per lo sviluppo individuale, ma anche per il progresso della società nella sua collettività.

[15] Romanian Constitutional Court, Judgement of 6 December 2024, no. 32. Si vedano D. VAIRA, *Trick or T(h)reat: disinformazione online e minacce ibride nel panorama europeo. Alcune considerazioni alla luce dell'annullamento delle elezioni in Romania*, in *SIDIBlog*, 29 dicembre 2024; R. VIORESCU, D. VARELA, *Constitutional Analysis of the Judgment of the Constitutional Court of Romania No. 32/2024 Annulling the Presidential Elections*, in *European Journal of Law and Public Administration*, 2024, pp. 243-260; L. DI ANSELMO, *La disinformazione online e i rischi per la democrazia: qualche considerazione sul ruolo del* Digital Services Act *alla luce delle elezioni presidenziali in romania*, in *Ordine internazionale e diritti umani*, 3/2025.

[16] Il 17 dicembre 2024 la Commissione europea ha avviato un procedimento formale nei confronti di *TikTok* per verificare se, nel contesto delle elezioni rumene, la piattaforma abbia rispettato gli obblighi ad essa incombenti ai sensi del DSA in materia di mitigazione dei rischi sistemici riguardanti il regolare svolgimento del

Nei casi più gravi, tali condotte possono arrivare ad integrare una violazione del principio di non ingerenza internazionale[17].

Non sorprende, dunque, che la strategia europea di contrasto alla disinformazione si sia concentrata principalmente sul contenimento dell'impatto di influenze di matrice esterna, particolarmente in ambiente digitale.

È invero da rilevare che, in un simile scenario, pratiche consolidate nell'ambito *offline* – come il *gerrymandering* politico[18], ossia la manipolazione strategica dei confini elettorali tramite tecniche di *packing* e *cracking* – assumono, *mutatis mutandis*, una nuova e più insidiosa dimensione nell'ecosistema digitale. Ciò in quanto, se nel contesto tradizionale il *gerrymandering* si realizza attraverso la ridefinizione territoriale di distretti elettorali fisici in un numero determinato e limitato, in ambito digitale la segmentazione degli elettori avviene attraverso frontiere non visibili, modellate dagli algoritmi sulla base delle interazioni e dei dati personali raccolti *online*, con una portata molto più estesa e pervasiva. Tale redistribuzione virtuale della popolazione, che può essere opportunamente descritta come *gerrymandering* digitale, da intendersi come la manipolazione degli spazi informativi e dei flussi algoritmici per influenzare selettivamente la visibilità politica degli utenti, consente pratiche avanzate di *microtargeting* e *retargeting* politico, con la conseguente esposizione mirata di gruppi specifici a determinati messaggi e la possibile esclusione di altri segmenti dall'arena informativa e partecipativa. Ne deriva un rischio di alterazione sistematica dell'equità della competizione democratica, che può realizzarsi attraverso l'azione poco trasparente di piattaforme e algoritmi, capaci di replicare, e talvolta accentuare, le distorsioni già note del sistema rappresentativo[19]. In un simile contesto, ciò che può emergere è una nuova forma di manipolazione del consenso – difficilmente regolabile e spesso opaca – che può incidere negativamente sull'imparzialità dei processi elettorali. Tale imparzialità rappresenta una precondizione imprescindibile per la tutela dell'ordine democratico, nel quale le regole e i flussi informativi che sostengono la competizione politica non devono garantire vantaggi sistematici ad alcun soggetto. Solo così è possibile assicurare pari opportunità di partecipazione, la libera formazione delle preferenze e decisioni collettive che rispecchino realmente la volontà pubblica, anziché gli interessi di posizioni di potere consolidate. In assenza di tali garanzie, si rischia di alimentare divisioni nell'elettorato e di alterare l'uguaglianza sostanziale nell'accesso alle informazioni.

Trovandosi di fronte a sfide tanto complesse, l'Unione europea, nel tentativo di contrastare il fenomeno della disinformazione, ha adottato strategie progressivamente più articolate[20]. A partire dalla prima fase, avviata nel 2015 con lo scoppio del conflitto russo-

processo elettorale. Si vedano J. ALBERT, *TikTok and the Romanian elections: A stress test for DSA enforcement*, in *DSA Observatory*, 20 December 2024; J. BARATA, E. LAZĂR, *Will the DSA Save Democracy? The Test of the Recent Presidential Election in Romania*, in *Tech Policy Press*, 27 January 2025; A. IANNOTTI DELLA VALLE, *Libertà di espressione e valori democratici alla prova dei social media: il DSA e un nuovo caso TikTok europeo*, in *federalismi.it*, n. 13/2025, pp. 84-101.

[17] La stessa Commissione nella Comunicazione sul *Piano d'azione per la democrazia europea*, cit., ha riconosciuto che la crescente digitalizzazione delle campagne elettorali e l'uso delle piattaforme *online* hanno esposto i processi democratici a nuove forme di manipolazione, disinformazione e vulnerabilità, tra cui finanziamenti opachi, l'*hacking* o il *defacing* di siti *web*, attacchi informatici alle infrastrutture elettorali e diffusione di messaggi polarizzanti tramite algoritmi poco trasparenti.

[18] Il termine deriva dal governatore E. Gerry, che all'inizio del XIX secolo, ridisegnò i confini elettorali del Massachusetts in modo irregolare per favorire la propria rielezione, includendo le aree a lui favorevoli ed escludendo quelle ostili.

[19] E. JORDAN, *How Computers turned Gerrymandering Into a Science*, in *New York Times*, 6 ottobre 2017.

[20] Si veda, O. POLLICINO, P. DUNN, *Intelligenza artificiale e democrazia*, cit., p. 129 ss.

ucraino, incentrata sulla risposta alla propaganda filorussa tramite la *East StratCom Task Force*[21], si è passati a una stagione di *soft law* inaugurata dalla comunicazione della Commissione dell'aprile 2018[22], che ha coinvolto le piattaforme *online* con il Codice di buone pratiche[23] e il sostegno all'autoregolamentazione. Constatata però la frammentazione normativa a livello nazionale[24] e l'inefficacia di tali iniziative, si è infine giunti a prediligere un approccio regolatorio più incisivo e armonizzato, segnato dall'adozione di strumenti come il *Digital Services Act* (DSA), il *Political Advertising Regulation* (PAR) e l'*AI Act*, che si esamineranno nel prosieguo, o di ulteriori atti fondamentali come il *Media Freedom Act* e il *Data Act*, su cui però non è possibile soffermarsi in questa sede.

3. *Il quadro giuridico europeo di riferimento:* DSA, PAR *e* AI Act *alla luce della Carta dei diritti fondamentali*

L'Unione europea, pur nel rispetto delle identità nazionali degli Stati membri[25], annovera il principio democratico tra i propri valori fondamentali[26], riconoscendolo quale criterio guida dell'azione di governo europea[27]. Con l'entrata in vigore del Trattato di Lisbona, il principio democratico trova una declinazione rafforzata nella complementarità tra democrazia rappresentativa e partecipativa, come sancito agli articoli 10 e 11 TUE. Questa impostazione riflette la consapevolezza che la democrazia rappresentativa, pur rimanendo imprescindibile, non sia da sola sufficiente a garantire la piena attuazione del fondamento

[21] La East StratCom Task Force (ESCTF) è un'unità istituita all'interno del Servizio europeo per l'azione esterna, incaricata di sviluppare strategie di comunicazione volte a rendere più efficace la diffusione e la promozione delle politiche e dei valori dell'Unione Europea nei Paesi dell'Europa orientale – comprendendo anche Armenia, Azerbaigian, Bielorussia, Georgia, Moldova e Ucraina – e, più in generale, nell'area che include anche la Russia. Dal 2022, il suo mandato si è ampliato fino a includere attività di contrasto e verifica delle campagne di disinformazione provenienti dalla Cina. Il progetto più importante di questa task force è *EUvsDisinfo*, un sito *web*, in tredici lingue, che include un database di articoli e media che ESCTF ha valutato che forniscano informazioni false, distorte o parziali nel loro contenuto, reperibile *online*.

[22] Comunicazione della Commissione, COM/2018/236 final del 26 aprile 2018, *Contrastare la disinformazione online: un approccio europeo*.

[23] Codice di buone pratiche dell'UE sulla disinformazione, 20 settembre 2018. Si veda sul punto M. MONTI, *The EU Code of Practice on Disinformation and the Risk of the Privatisation of Censorship*, in S. GIUSTI, E. PIRAS (a cura di), *Democracy and Fake News: Information Manipulation and Post-Truth Politics*, Londra, 2020, pp. 214-225; G. MORGESE, *Il contrasto alla disinformazione originata da ingerenze straniere nell'Unione europea*, in M. Messina (a cura di), *Cittadinanza e stato di diritto per un'unione europea più forte*, Napoli, 2024, p. 89 ss.

[24] Da menzionare il *Netzwerkdurchsetzungsgesetz*, *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* volto a contrastare la diffusione di contenuti illeciti in rete si veda V. CLAUSSEN, *Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European Legislation*, in *Rivista del diritto dei media*, 3, pp. 110-136.

[25] Art. 4, par. 2 TUE.

[26] Art. 2 TUE. Si vedano A. PIZZORUSSO, *Il patrimonio costituzionale europeo*, Bologna 2002; U. VILLANI, *Istituzioni di diritto dell'Unione europea*, Bari, 2024, 7° ed., p. 43 ss. La Corte di giustizia, nelle note sentenze gemelle in materia di tutela dello Stato di diritto, causa C-156/21, *Ungheria c. Parlamento europeo e Consiglio*, sentenza del 16 febbraio 2022; causa C-157/21, *Polonia c. Parlamento europeo e Consiglio*, sentenza del 16 febbraio 2022, ha definito questi valori come espressione dell'essenza stessa dell'identità costituzionale europea.

[27] Sul punto si veda G. ZACCARONI, *Intelligenza artificiale e principio democratico: riflessioni a margine dell'emersione di un quadro normativo europeo*, in *Quaderni AISDUE*, 2/2024.

democratico dell'integrazione europea, rendendo necessario il rafforzamento degli strumenti di partecipazione diretta dei cittadini al processo decisionale dell'Unione[28].

Eppure, gli sforzi compiuti a livello europeo rischiano di essere vanificati dall'emergere di nuove tecnologie e dalle pratiche, talvolta esplicite e talora meno visibili, riconducibili a quella forma di *gerrymandering* digitale richiamata in precedenza, che finisce per attribuire un potere sproporzionato a chi dispone delle risorse per impiegare sofisticati strumenti di *targeting* o sfruttare i *bias* inevitabilmente presenti nei sistemi.

Un dato appare, infatti, incontrovertibile, il panorama digitale rimane saldamente nelle mani delle *Tech Giants*, quasi sempre con sede in Stati terzi, che hanno consolidato prassi di autoregolamentazione e imposto regole proprie, spesso al di fuori dei circuiti democratici[29] e in costante competizione con i poteri pubblici. Questo scenario pone un duplice rischio: da un lato, le piattaforme possono esercitare un'influenza determinante sulle scelte collettive; dall'altro, possono adottare forme di censura discrezionale sui contenuti, con effetti potenzialmente lesivi della libertà di espressione e delle dinamiche democratiche[30]. In tale contesto, il principio di *net neutrality* – originariamente di natura tecnica – assume una rilevanza giuridica crescente, considerando che le regole della rete vengono dettate unilateralmente dalle piattaforme, che però per lungo tempo, non sono state ritenute responsabili dei contenuti immessi in rete[31].

In un simile quadro eterogeneo, le politiche digitali europee si sono orientate nella direzione di un approccio regolatorio rinnovato[32] volto a superare la tradizionale logica di intervento verticale e settoriale a favore di una regolamentazione più orizzontale e trasversale[33].

Il primo strumento che, nella prospettiva della presente analisi, appare opportuno esaminare è il DSA[34]. L'obiettivo del regolamento è quello di assicurare un ambiente digitale sicuro e affidabile, in cui risultino garantiti i diritti riconosciuti dalla Carta dei diritti fondamentali[35] attraverso una disciplina articolata della moderazione dei contenuti e l'introduzione di un complesso di regole e procedure volte ad assicurare il rispetto dei principi

---

[28] Sul punto si veda G. MORGESE, *Principio e strumenti della democrazia partecipativa nell'Unione europea*, in E. Triggiani (a cura di), *Le nuove frontiere della cittadinanza europea*, Bari, 2011, p. 37 ss.

[29] Cfr. M. MONTI, *Privatizzazione della censura e Internet Platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, in *Rivista italiana di informatica e diritto*, 1/2019, p. 37 ss; M. BETZU, *I baroni del digitale*, Napoli, 2022, p. 34 ss. Si veda altresì la pronuuncia della US Supreme Court, *Biden v. Knight First Amend. Inst. at Colum. Univ.*, No. 20-197, 5 April 2021, (J. Thomas, concurring opinion), 141 S. Ct. at 1222.

[30] Si vedano, *ex multis*, M. MANETTI, *Regolare Internet*, in *MediaLaws*, 2/2020, p. 36 ss.; M. BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, in *Rivista del Gruppo di Pisa*, 2/2021, p. 172 ss.

[31] Si veda M. C. GIRARDI, *Libertà e limiti della comunicazione nello spazio pubblico digitale*, in *federalismi.it*, 2024.

[32] Per una ricognizione del quadro giuridico generale si veda G. CAGGIANO, *Il quadro normativo del mercato unico digitale*, in *Eurojus*, fascicolo speciale *Mercato Unico Digitale, dati personali e diritti fondamentali*, (a cura di) F. Rossi Dal Pozzo, 2020, p. 13 ss.

[33] O. POLLICINO, P. DUNN, *Intelligenza artificiale e democrazia*, cit., p. 129 ss.

[34] Regolamento (UE) 2022/2065 del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali). Sul tema disinformazione e DSA si vedano, *ex multis*, E. BIRRITTERI, *Contrasto alla disinformazione, Digital Services Act e attività di private enforcement: fondamento, contenuti e limiti degli obblighi di compliance e dei poteri di autonormazione degli operatori*, in *MediaLaws*, 2/2023, p. 73; L. D'AGOSTINO, *Disinformazione e obblighi di compliance degli operatori del mercato digitale alla luce del nuovo Digital Services Act*, in *MediaLaws*, 2/2023, p. 33 ss.; N. ZINGALES, *The DSA as a Paradigm Shift for Online Intermediaries' Due Diligence*, in J. VAN HOBOKE, J.P. QUINTAIS, N. APPELMAN, R. FAHY, I. BURI, M. STRAUB (eds.), *Putting the DSA into Practice. Enforcement, Access to Justice and Global Implications*, Berlin, 2023, p. 211 ss.

[35] Sul tema della salvaguardia dei diritti fondamentali e del loro bilanciamento si veda estensivamente F. FERRI, *Il bilanciamento dei diritti fondamentali nel mercato unico digitale*, Torino, 2022.

di legalità, trasparenza e limitazione della discrezionalità dei fornitori di servizi *online*[36]. Attraverso specifiche misure di filtraggio, linee guida e protocolli, il DSA mira a creare un quadro normativo europeo uniforme, distinguendo chiaramente le responsabilità dei fornitori di servizi. Il regolamento introduce severi obblighi di trasparenza e una definizione di "moderazione dei contenuti"[37], imponendo alle piattaforme di pubblicare dettagli sui criteri e parametri utilizzati, pur mantenendo il regime di esonero dalla responsabilità diretta dei *provider*. L'ambito di applicazione si estende a tutti i servizi di intermediazione destinati a utenti nell'Unione europea, indipendentemente dalla sede del fornitore, purché esista un rapporto significativo con i destinatari[38]. Inoltre, i fornitori sono tenuti a rispettare obblighi di vigilanza graduati in funzione del servizio e delle dimensioni dell'intermediario. Nello specifico, VLOPs e VLOSEs sono soggetti sia agli obblighi generali, sia a requisiti aggiuntivi, tra cui la pubblicazione delle *policy* e delle procedure di moderazione – algoritmica e umana –, nonché la predisposizione di *report* periodici sulle attività svolte. Il DSA accresce altresì le tutele per gli utenti, consentendo di segnalare contenuti illeciti e imponendo alle piattaforme trasparenza nelle raccomandazioni e nella pubblicità, e vietando pratiche ingannevoli nella gestione delle interfacce[39]. Mira, inoltre, a garantire la piena consapevolezza circa le opzioni a disposizione nell'utilizzo dei servizi *online*, anche mediante procedure di *disclaimer*[40] e richiede alle piattaforme di rendere noti i parametri utilizzati nei sistemi di raccomandazione e di indicare chiaramente quando un contenuto costituisce pubblicità, specificando *sponsor* e committenti[41].

Permangono, tuttavia, alcune criticità nell'impianto sanzionatorio delineato dal DSA che si configura come un sistema multilivello fondato sulla combinazione tra competenze nazionali e poteri centralizzati in capo alla Commissione. Agli Stati membri è attribuito il compito di definire e applicare le sanzioni nei confronti della generalità dei fornitori di servizi intermediari, elaborando regimi nazionali che garantiscano effettività, proporzionalità e dissuasività[42]. La Commissione, invece, assume un ruolo diretto e centrale nei confronti delle piattaforme *online* e dei motori di ricerca di dimensioni molto grandi, sui quali esercita poteri investigativi autonomi e può irrogare sanzioni pecuniarie di particolare rilevanza. Proprio questa ripartizione di competenze tra livello europeo e nazionale genera però il rischio di applicazioni disomogenee, alimentando disparità tra ordinamenti e asimmetrie tra operatori "sistemici" e non, con possibili effetti negativi sulla coerenza del sistema e sulla tutela uniforme degli utenti.

Come precedentemente evidenziato, un ulteriore elemento di primaria importanza per la salvaguardia dell'assetto democratico concerne la disciplina della pubblicità politica, ambito nel quale si assiste a un crescente impiego di sofisticate tecniche di profilazione degli utenti.

---

[36] Si vedano O. POLLICINO, G. DE GREGORIO, M. BASSINI, *Verso il Digital Services Act: problemi e prospettive. Presentazione del simposio*, in *MediaLaws*, 23 novembre 2020; G. CAGGIANO, *Il contrasto alla disinformazione tra nuovi obblighi delle piattaforme online e tutela dei diritti fondamentali nel quadro del* Digital Service Act *e della co-regolamentazione*, in *Papers di diritto europeo*, 2021, pp. 45-72 e G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea sui mercati digitali*, Bari, 2021.

[37] Art. 3, par. 1, lett. t).

[38] Si veda F. MAROGIU BUONAIUTI, *L'ambito di applicazione territoriale del* Digital Markets Act *e del* Digital Services Act, in G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea sui mercati digitali*, cit., p. 171 ss.

[39] Art. 25 DSA.

[40] Art. 15, par. 1, lett. e) DSA.

[41] Art. 26 DSA. Si veda 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*, 2/2021, p. 14 ss.

[42] Art. 52 DSA.

Tali strumenti consentono l'invio di messaggi personalizzati e mirati, finalizzati a massimizzare l'efficacia persuasiva della comunicazione politica e a incidere in modo più determinante sulla formazione del consenso elettorale[43].

L'Unione europea ha alzato il livello di attenzione sul tema della disinformazione dopo i casi delle elezioni USA 2016 e della *Brexit*, raccomandando l'adozione di misure specifiche[44]. Tale impegno si è concretizzato nell'adozione del regolamento sulla trasparenza e il *targeting* della pubblicità politica (PAR)[45], adottato sulla base degli articoli 16 e 114 TFUE. Il PAR introduce standard uniformi in materia di trasparenza, obblighi di *due diligence* e gestione dei dati per la pubblicità politica, regolamentando in particolare l'impiego di tecniche di *targeting* fondate sul trattamento di dati personali. Prevede inoltre l'istituzione di un archivio pubblico accessibile, volto a garantire la tracciabilità e la pubblicità delle inserzioni politiche *online* diffuse nell'Unione europea[46].

All'interno del regolamento viene proposta una definizione di "pubblicità politica" particolarmente estesa, che si sviluppa su due livelli: soggettivo, includendo non solo partiti, candidati e attori istituzionali, ma anche *sponsor*, editori e piattaforme coinvolte; ed oggettivo, considerando come pubblicità politica qualsiasi messaggio, a prescindere dal soggetto promotore, che possa influenzare un'elezione, un *referendum* o un processo legislativo a qualsiasi livello[47]. Ne consegue che una comunicazione può assumere la natura di pubblicità politica sia in ragione dello *sponsor*, sia in considerazione degli effetti perseguiti, come accade, ad esempio, per le cosiddette *issue-based ads* o *social issue ads*. Questa ampiezza definitoria comporta il rischio di ricomprendere anche forme di comunicazione non strettamente politiche, come l'attivismo sociale, il giornalismo o le semplici espressioni civiche, sollevando così dubbi sulla possibilità di restrizioni eccessive alla libertà di espressione.

Al centro del PAR vi sono gli obblighi di identificazione e trasparenza delle inserzioni politiche[48]. Come visto nel caso del DSA[49], anche nel PAR la trasparenza assume un rilievo fondamentale[50] per rendere la pubblicità politica più facilmente riconoscibile, con una probabile riduzione dei fenomeni di disinformazione e altre manipolazioni. A motivo di ciò, ogni pubblicità politica deve recare un'etichetta identificativa, accompagnata da una nota di trasparenza che indichi i dettagli relativi allo *sponsor* dell'annuncio e al procedimento elettorale di riferimento. Viene richiesta la comunicazione di informazioni sia al pubblico in generale, sia alle autorità di regolamentazione, sia agli utenti destinatari delle singole inserzioni e agli altri soggetti interessati[51]. Le piattaforme di grandi dimensioni sono soggette a obblighi aggiuntivi di segnalazione e gestione delle notifiche riguardanti inserzioni non conformi[52].

---

43 Particolarmente significative sono pratiche promosse negli Stati Uniti come il *voter isolation* e la commercializzazione di database elettorali da parte di società come Aristotle International - che ha venduto dati su 150 milioni di elettori per scopi di marketing e propaganda politica - hanno sollevato ampie discussioni sul rischio di sfruttamento e manipolazione dei dati personali in ambito elettorale.

44 Si veda per approfondimenti M. Z. VAN DRUNEN, N. HELBERGER, R. Ó FATHAIGH, *The Beginning of EU Political Advertising Law: Unifying Democratic Visions through the Internal Market*, in *International Journal of Law and Information Technology*, 2022, p. 181 ss.

45 Regolamento (UE) 2024/900 del 13 marzo 2024 relativo alla trasparenza e al *targeting* della pubblicità politica.

46 Art. 1 par. 1 PAR.

47 Art. 3 par. 2 e considerando 22 e 23 PAR.

48 Artt. 7 e 15 e si vedano altresì i considerando 44 e 54 PAR.

49 Articoli 26 e 39 DSA.

50 Art. 6, par. 1 PAR.

51 Art. 11, par. 1 e art. 12 PAR.

52 Si veda S. ESKENS, *The role of the Political Advertising Regulation and European Media Freedom Act in the EU's anti-disinformation approach*, *Working Paper*, 31 August 2024, reperibile *online*.

Si aggiunga che, opportunamente, il PAR limita l'uso delle strategie di *targeting* e *ad-delivery*[53]. Tali pratiche sono consentite solo previo consenso esplicito dell'interessato[54], esclusa la profilazione su dati sensibili, come prescritto anche nel DSA. Rimane tuttavia incerto se il PAR consenta forme di *targeting* che, pur non prevedendo la profilazione, si basino comunque su dati sensibili. Queste restrizioni intendono prevenire la manipolazione e le interferenze tramite l'uso delle vulnerabilità dei singoli soggetti, posto che il trattamento dei dati personali a fini di pubblicità politica può incidere negativamente sui diritti e sulle libertà individuali, oltre a rappresentare un potenziale rischio per il corretto funzionamento del processo democratico.

I titolari del trattamento sono, inoltre, tenuti a garantire il massimo livello di trasparenza nell'impiego di algoritmi e sistemi di IA utilizzati per il *targeting* pubblicitario, adottando *policy* chiare e informando gli utenti circa i criteri adottati. Tale obbligo si pone, ancora una volta, in continuità con quanto previsto da DSA[55] e, in questo caso, anche dal GDPR[56], che impongono di informare gli interessati in merito alle logiche sottese alle decisioni automatizzate e ai principali parametri impiegati nei sistemi di raccomandazione e di pubblicità.

Si prevede che la Commissione istituisca un archivio pubblico delle inserzioni politiche *online* diffuse nell'Unione, diretti a cittadini europei o residenti[57]. Inoltre, al fine di adempiere agli obblighi previsti dal PAR, i fornitori di pubblicità politica che, ai sensi del DSA, sono considerati VLOPs o VLOSEs, dovranno garantire la disponibilità e la trasparenza di tali inserzioni sia tramite tale archivio europeo sia attraverso propri registri esistenti[58].

Benché il quadro normativo risulti articolato e meritevole di apprezzamento, permangono nondimeno alcune criticità. Sebbene, infatti, il PAR persegua la trasparenza delle inserzioni politiche, affida la responsabilità primaria di identificazione allo *sponsor*, imponendo alle piattaforme digitali requisiti solo minimi in materia di controllo. Questa impostazione potrebbe consentire agli inserzionisti che operano in maniera non trasparente di eludere facilmente gli obblighi di legge, omettendo semplicemente la dichiarazione della natura politica dell'annuncio e aggirando così i meccanismi di trasparenza e rendicontazione previsti. L'assenza di incisivi obblighi di *due diligence* per le piattaforme espone il sistema al rischio di manipolazione informativa, soprattutto nei casi di utilizzo illecito dei dati personali o di discrepanza tra fondi impiegati e dichiarati. In tale contesto, il fenomeno dei 'falsi negativi' – ovvero annunci politici non riconosciuti né dalla piattaforma, né dallo *sponsor* – sottolinea la necessità di rafforzare gli obblighi di identificazione su entrambi i fronti.

Alla mitigazione di una simile criticità potrebbe in parte soccorrere il DSA che, sotto il profilo della trasparenza, offre un quadro di tutela più integrato, imponendo alle VLOPs e ai VLOSEs obblighi specifici di valutazione e mitigazione dei rischi sistemici, inclusa la mancata identificazione delle inserzioni politiche. In questo senso, particolarmente rilevanti sono le disposizioni che qualificano come rischi sistemici i danni al dibattito pubblico e alle procedure elettorali, imponendo misure correttive sulle modalità di diffusione degli annunci[59]. Nella stessa prospettiva, appare centrale anche l'obbligo per le grandi piattaforme

[53] Considerando 77 PAR.
[54] Art. 4 GDPR.
[55] Art. 39 par. 1, lett. f) DSA.
[56] Art. 22 GDPR.
[57] Art. 13, par. 1, PAR.
[58] Art. 13, par. 2 e art. 16 PAR.
[59] Articoli 34 e 35 DSA.

di istituire e pubblicare un registro degli annunci pubblicitari, comprensivo di informazioni sui criteri di *targeting* e sulla profilazione degli utenti. Questo sistema di trasparenza rafforzata può contribuire a rendere più chiari anche i meccanismi sottesi alla pubblicità politica, limitando il rischio di manipolazione e garantendo una maggiore *accountability* degli intermediari digitali.

Va rilevato che la complessità dell'ecosistema digitale è ulteriormente accresciuta dal fatto che il funzionamento delle piattaforme si fonda in larga misura su sistemi algoritmici. Questo rende imprescindibile, nell'ottica della presente disamina, anche alcune considerazioni in merito alla disciplina contenuta all'interno del regolamento sull'intelligenza artificiale (*AI Act)*. Tali sistemi, infatti, si prestano a molteplici usi potenzialmente lesivi della qualità del dibattito pubblico, favorendo la produzione automatizzata di contenuti disinformativi e, in alcuni casi, anche di *output* frutto di cosiddette 'allucinazioni', ossia informazioni meramente misinformative[60].

Si tratta di un atto notoriamente complesso, il cui esame di dettaglio esula dalla presente disamina, nondimeno per ciò che riguarda la tutela dell'assetto democratico l'*AI Act* si affida eminentemente a due strumenti, uno di natura trasversale e orizzontale, che si sostanzia nell'approccio basato sul rischio – attraverso il quale si vietano o si sottopongono a obblighi stringenti i sistemi con portata lesiva particolarmente alta – e l'altro, più specifico, ovvero la valutazione dell'impatto sui diritti fondamentali, sulla democrazia e lo Stato di diritto[61]. Il sistema di gestione del rischio delineato dall'*AI Act*, articolato nelle quattro fasi di identificazione e analisi, valutazione, monitoraggio successivo all'immissione sul mercato e adozione delle misure di mitigazione, si propone come risposta normativa alle minacce dell'IA per l'assetto democratico, rafforzandosi nel coordinamento con strumenti orizzontali come i già esaminati DSA e PAR. Pur sussistendo alcuni profili di non piena coerenza normativa, il quadro così delineato mira a bilanciare tutela dei diritti individuali e salvaguardia degli interessi pubblici fondamentali, tra cui la democrazia.

La centralità di questi valori emerge chiaramente già dalla parte introduttiva del regolamento: nei consideranda 1, 2 e 8 si sottolinea la necessità che l'intelligenza artificiale rispetti i valori europei; nei consideranda 61 e 62 si richiama l'attenzione sui rischi legati ai sistemi di IA ad alto rischio nei processi democratici e giudiziari, mentre il considerando 120 evidenzia l'importanza del coordinamento con il DSA, soprattutto in relazione ai rischi per il dibattito pubblico e i processi elettorali.

Sul piano operativo, il sistema di gestione del rischio per i sistemi di IA ad alto rischio, disciplinato dall'art. 9, deve accompagnare l'intero ciclo di vita dell'IA e si articola in quattro fasi fondamentali: identificazione e analisi dei rischi per la salute, la sicurezza e i diritti fondamentali; valutazione e stima dei rischi derivanti da un uso improprio; monitoraggio dei rischi successivi all'immissione sul mercato; adozione di misure appropriate per mitigarli. Si tratta di un processo dinamico e ininterrotto che impone aggiornamenti e revisioni costanti, e che riflette la volontà del legislatore europeo di garantire un elevato livello di salvaguardia, soprattutto nei confronti dei soggetti più deboli.

---

[60] Per allucinazione algoritmica si intende la produzione, da parte di un modello computazionale, di *output* non aderenti ai dati, di contenuti non verificati o non supportati, risultanti da errori di generalizzazione, insufficienze del *training set* utilizzati o limiti nei meccanismi di inferenza. Si veda la Communication to the Commission, 26.3.2024 C(2024) 2121 final, *Approval of the content of a draft Communication from the Commission on Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to the Digital Services Act (Regulation (EU) 2022/2065).*

[61] G. ZACCARONI, *Intelligenza artificiale e principio democratico*, cit., p. 23 ss.

Un ulteriore elemento di rafforzamento della tutela è rappresentato dall'art. 27, il quale impone agli enti pubblici, agli enti privati che offrono servizi di interesse pubblico e ai *deployer* di sistemi di IA ad alto rischio in determinati settori, l'obbligo di effettuare una valutazione d'impatto sui diritti fondamentali anteriormente al primo utilizzo del sistema. Tale valutazione, concepita per identificare e prevenire potenziali impatti negativi sull'esercizio dei diritti garantiti dalla Carta dei diritti fondamentali dell'Unione europea, inclusi il principio democratico e lo Stato di diritto, deve descrivere le misure di mitigazione e sorveglianza adottate e prevedere azioni correttive in caso di danni. L'obbligo si applica soprattutto ai soggetti che utilizzano l'IA in ambiti sensibili e la valutazione va notificata all'autorità di vigilanza, potendo essere integrata con le valutazioni d'impatto *privacy* già previste dalla normativa europea.

In linea con questi obiettivi, l'art. 74, par. 8, stabilisce che, nei settori particolarmente sensibili per la vita democratica – come l'attività di contrasto, la gestione delle frontiere, la giustizia e la stessa democrazia – l'utilizzo di sistemi di intelligenza artificiale ad alto rischio sia soggetto a una vigilanza rafforzata da parte delle autorità nazionali per la protezione dei dati personali o di altri organismi dotati delle necessarie garanzie di indipendenza. Al tempo stesso, si tutela esplicitamente l'autonomia del potere giudiziario, quale presidio imprescindibile dello Stato di diritto, escludendo espressamente qualsiasi forma di interferenza. Inoltre, l'art. 77 attribuisce alle autorità pubbliche nazionali incaricate della tutela dei diritti fondamentali il potere di accedere a tutta la documentazione sui sistemi di IA ad alto rischio, chiedere verifiche tecniche, ove necessario, e coordinarsi con le autorità di vigilanza del mercato, rafforzando così le garanzie di trasparenza, *accountability* e controllo democratico.

Nel complesso, dunque, l'approccio delineato dall'*AI Act* pone l'accento sulla necessità di garantire un bilanciamento tra la promozione dell'innovazione e la salvaguardia dell'assetto democratico. Tuttavia, tale impostazione non è esente da criticità, poiché richiede di contemperare spinte regolatorie ed esigenze di sviluppo senza compromettere, da un lato, la competitività del settore e, dall'altro, la tutela dei diritti fondamentali e delle dinamiche istituzionali che sostengono il sistema democratico.

4. *Conclusioni*

Alla luce di quanto sopra, alcune riflessioni conclusive possono svolgersi in punto di coerenza normativa e di coordinamento degli atti esaminati. In assenza di procedure integrate e di meccanismi di raccordo efficaci, il quadro giuridico delineato rischia di lasciare spazi di tutela scoperti proprio su aspetti essenziali per la protezione della democrazia, come la prevenzione di *deepfake* elettorali e la manipolazione automatizzata del consenso. A ciò si sommano le incertezze sulla ripartizione delle competenze tra autorità nazionali, Commissione europea e nuove strutture di supervisione, con il rischio che l'azione di tutela risulti frammentata o, al contrario, eccessivamente burocratizzata e, dunque, poco tempestiva.

Sotto un'altra prospettiva, l'*AI Act* – così come il PAR – solleva il delicato problema del bilanciamento tra il contrasto alle forme più insidiose di manipolazione digitale e la salvaguardia della libertà di espressione e del pluralismo del dibattito pubblico, filtri automatizzati e restrizioni non adeguatamente calibrati rischiano, infatti, di comprimere

ingiustificatamente lo spazio del confronto democratico. Il DSA, pur fissando obblighi di trasparenza e gestione responsabile dei contenuti, risulta troppo generico sulla pubblicità politica, lasciando ampi margini di discrezionalità alle piattaforme. Il PAR colma solo parzialmente questo vuoto, imponendo requisiti di etichettatura e trasparenza, ma demandando quasi integralmente agli *sponsor* la qualificazione delle inserzioni come politiche, mentre i controlli a carico delle piattaforme restano minimi, rende agevole, per chi voglia eludere il sistema, aggirare le misure di trasparenza semplicemente omettendo di dichiarare la natura politica di un messaggio.

Non meno significativo, nella prospettiva qui adottata, è il fatto che l'*AI Act*, nonostante l'ambizione di presidiare i rischi che le tecnologie di intelligenza artificiale possono comportare per i processi democratici, soffre di una certa indeterminatezza nella definizione di cosa costituisca effettivamente un "rischio per la democrazia". Questa vaghezza si traduce, ancora una volta, in una eccessiva discrezionalità affidata sia alle autorità di vigilanza sia agli operatori di mercato, con il rischio di produrre applicazioni disomogenee a livello nazionale.

Va ricordato inoltre che gli stringenti obblighi di gestione e valutazione del rischio, nonché di monitoraggio continuo, imposti alle IA ad alto rischio, risultano particolarmente onerosi, soprattutto per operatori di piccole dimensioni. Ne consegue che soltanto i grandi operatori sono realisticamente in grado di sostenere i costi della *compliance*, con la potenziale conseguenza di una riduzione del pluralismo informativo e, indirettamente, di un indebolimento delle garanzie democratiche. Inoltre, la disciplina sul *risk management* introdotta dall'*AI Act* fatica a coordinarsi in modo sistematico con le previsioni del DSA e del PAR, in particolare rispetto alla trasparenza algoritmica e alla gestione delle segnalazioni di contenuti illeciti o manipolativi. Quanto al primo profilo, il DSA prevede la spiegazione delle logiche algoritmiche per la raccomandazione dei contenuti; il PAR esige etichettatura e note di trasparenza per ogni inserzione politica; tuttavia la responsabilità di verifica è suddivisa tra più attori e la mancanza di controlli effettivi lato piattaforma può lasciare ampi spazi di opacità. Analogamente, i sistemi di segnalazione risultano frammentati tra i tre regolamenti e la possibilità di un intervento tempestivo su contenuti manipolativi o pubblicità non dichiarate resta limitata, soprattutto per i piccoli *publisher* o per i casi in cui l'IA impiegata non sia espressamente "ad alto rischio".

Questa segmentazione rischia di avere un impatto negativo non solo sulla coerenza del sistema, ma soprattutto sulla tutela effettiva della democrazia e dei diritti fondamentali. Pratiche come il *microtargeting*, la profilazione spinta e l'utilizzo distorto degli algoritmi possono portare a una banalizzazione del dibattito pubblico, a una selezione degli interlocutori politici sempre più ristretta e alla progressiva esclusione delle minoranze dai processi comunicativi. Ciò potrebbe condurre ad un'erosione del pluralismo e del principio democratico, aggravata dal rischio che soggetti dotati di mezzi quasi illimitati e del controllo su piattaforme influenti possano polarizzare il discorso pubblico, manipolando l'opinione collettiva anche attraverso pratiche riconducuibili al precedentemente delineato *gerrymandering* digitale.

Il contemperamento dei diversi interessi in gioco resta però fondamentale poiché, in senso opposto, il crescente ricorso a procedure automatizzate di moderazione, se non adeguatamente supervisionato, rischia di comprimere in modo irragionevole la libertà di espressione. Vi è, infatti, il pericolo che filtri algoritmici non distinguano correttamente tra manifestazioni di legittimo dissenso politico e contenuti realmente manipolativi. Ciò può

tradursi in forme di censura arbitraria o, al contrario, in un'insufficiente rilevazione di contenuti lesivi del dibattito democratico.

In prospettiva giuridica, si pone, dunque, in termini particolarmente stringenti il tema del bilanciamento e della proporzionalità, poiché – come affermato anche dalla Corte europea dei diritti dell'uomo[62] – eventuali restrizioni all'espressione politica sono legittime solo se necessarie e giustificate dalla necessità di tutelare effettivamente il processo democratico. L'attuale assetto regolatorio rischia, invece, di introdurre limitazioni indifferenziate, idonee ad incidere anche su iniziative civiche e comunicazioni di interesse pubblico, compromettendo così il nucleo essenziale delle libertà costituzionali.

Appare quindi urgente, per il futuro, rafforzare il coordinamento all'interno del delineato quadro normativo vigente, sviluppando procedure integrate di controllo, interoperabilità dei sistemi di segnalazione e di trasparenza e meccanismi di *audit* congiunti tra autorità, piattaforme e *stakeholder*.

Solo un approccio realmente sinergico e multilivello potrà garantire una *governance* digitale in grado di affrontare le molteplici sfide, capace di tutelare la libertà di espressione, il pluralismo e la qualità della democrazia europea nell'era delle piattaforme e dell'intelligenza artificiale.

[62] Secondo la Corte EDU, elezioni libere e libertà di espressione costituiscono il fondamento di ogni democrazia. I due diritti sono tra loro interconnessi e si rafforzano reciprocamente, cfr., *ex multis*, *Orlovskaya Iskra c. Russia*, ric. n. 42911/08, sentenza del 21 febbraio 2017, par. 110. Tuttavia, in determinate circostanze, può essere necessario imporre alcune restrizioni alla libertà di espressione per garantire un giusto equilibrio, cfr. *Bowman c. Regno Unito*, ric. n. 141/1996/760/961, sentenza del 19 febbraio 1998, par. 43.