



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 Zanghi, Lina Panella, Carlo Curti Gialdino

EDITORIALE
SCIENTIFICA
MILANO

OSSERVATORIO NUOVE TECNOLOGIE E DIRITTI FONDAMENTALI

coordinato da Francesco Battaglia

N. 3
15 LUGLIO 2025



Co-funded by
the European Union



OSSERVATORIO NUOVE TECNOLOGIE E DIRITTI FONDAMENTALI N. 3/2025

1. LA DISINFORMAZIONE *ONLINE* E I RISCHI PER LA DEMOCRAZIA: QUALCHE CONSIDERAZIONE SUL RUOLO DEL *DIGITAL SERVICES ACT* ALLA LUCE DELLE ELEZIONI PRESIDENZIALI IN ROMANIA

1. *Introduzione*

Le recenti elezioni presidenziali in Romania hanno palesato la vulnerabilità della democrazia nell'era digitale. Il loro andamento, infatti, è stato fortemente influenzato da un'intensa mobilitazione *online* condotta da attori stranieri a sostegno del candidato indipendente, il nazionalista e filo-russo Călin Georgescu. Gli efficienti algoritmi che governano il funzionamento delle piattaforme digitali sono stati sfruttati per portare a compimento una campagna di disinformazione in grado di ribaltare le previsioni di voto (in generale su tali aspetti, cfr. O. POLLICINO, P. DUNN, *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi (ed opportunità)*, in [federalismi.it](https://www.federalismi.it), n. 12/2024, p. iv ss.). Nonostante i sondaggi della vigilia lo ritenessero tutt'altro che favorito, al primo turno Georgescu ha ottenuto la maggioranza relativa dei voti, pari al 22,94% dei consensi, tra lo stupore dell'opinione pubblica nazionale ed europea. Il 4 dicembre 2024, appena dieci giorni dopo le elezioni, un rapporto dei servizi segreti rumeni ha rilevato interferenze russe durante la campagna elettorale, condotte attraverso attività di propaganda e disinformazione *online*, soprattutto sulla piattaforma *social* TikTok. In sostanza, tali iniziative avrebbero avuto l'effetto di alterare il regolare svolgimento delle elezioni, giacché l'esposizione mediatica di Georgescu, unita all'impiego dell'intelligenza artificiale per scopi disinformativi, avrebbero condizionato le intenzioni di voto degli elettori. Alla luce di ciò, il 6 dicembre, a ridosso del ballottaggio tra Georgescu e la candidata liberale Elena Lasconi, la Corte costituzionale rumena ha annullato le elezioni in corso, stabilendo l'avvio di un processo elettorale *ex novo*.

La vicenda ha suscitato ampio interesse sia a livello mediatico che accademico, poiché chiama in causa due aspetti essenziali per la tenuta degli ordinamenti democratici: da un lato, l'esigenza di salvaguardare il legittimo interesse di uno Stato sovrano di impedire ingerenze straniere nei propri affari interni senza, al contempo, svuotare di significato la sovranità popolare; dall'altro, la consapevolezza della fragilità dei sistemi democratici di fronte alle minacce poste dalle tecnologie digitali.

Sotto il primo profilo, è logico che la decisione di annullare le elezioni, contravvenendo alla volontà popolare emersa dalle urne, rappresenti un intervento suscettibile di impattare in modo sostanziale sulle sorti di un ordinamento democratico. In ragione di ciò, la dottrina si è interrogata sulla legittimità della sentenza emessa dalla Corte rispetto al sistema

costituzionale rumeno (su tutti, cfr. D.A. CĂRĂMIDARIU, A. VERTEȘ-OLTEANU, *Safeguarding democracy: constitutional insights from Romania's election annulment*, in *Diritto pubblico comparato ed europeo*, 2025, pp. 139-165). In effetti, benché l'art. 146, lett. f), della costituzione rumena autorizzi la Corte a vigilare sul regolare svolgimento delle elezioni presidenziali, soltanto una violazione dei valori costituzionali fondamentali, *in primis* l'esercizio libero e incondizionato del diritto di voto, potrebbe comportare l'annullamento del procedimento elettorale. Nel caso di specie, ciò presupporrebbe l'esistenza di un nesso diretto tra l'interferenza russa esercitata su TikTok e l'esito del voto: ebbene, sostenere che qualora non vi fossero state azioni disinformative il risultato elettorale sarebbe stato diverso costituisce un'ipotesi verosimile, ma difficile da provare con certezza (al riguardo, cfr. E. SHATTOCK, *Electoral Dysfunction: Romania's Election Annulment, Disinformation, and ECHR Positive Obligations to Combat Election Irregularities*, in *EJIL: Talk!*, 6 January 2025).

Al di là di questi aspetti, sufficientemente esplorati altrove (cfr. B. SELEJAN-GUTAN, *The Second Round that Wasn't: Why The Romanian Constitutional Court Annulled the Presidential Elections*, in *Verfassungsblog*, 7 December 2024; K. CSONGOR, *On Means and Ends: The Annulment of the Romanian Presidential Elections*, in *Verfassungsblog*, 10 December 2024), il presente contributo intende soffermarsi sulla relazione intercorrente tra disinformazione e tenuta delle istituzioni democratiche nell'era digitale, da tempo al centro dell'agenda politica dell'Unione europea (in generale, cfr. A. KOLTAY, *Freedom of Expression and the Regulation of Disinformation in the European Union*, in R. J. KROTOSZYNSKI, A. KOLTAY, C. GARDEN (eds.), *Disinformation, Misinformation, and Democracy. Legal Approaches in Comparative Context*, Cambridge, 2025, pp. 133-160; 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.; S. SASSI, *L'Unione Europea e la lotta alla disinformazione online*, in *federalismi.it*, n. 15/2023, pp. 183-201).

Pur senza essere oggetto di una regolamentazione specifica, infatti, il contrasto alla disinformazione ha trovato spazio nell'ambito del *Digital Services Act*, il quale, come noto, pur basandosi sul consolidato principio, ereditato dalla c.d. *direttiva e-commerce*, della tendenziale irresponsabilità dei prestatori dei servizi di intermediazione digitale per i contenuti diffusi da soggetti terzi attraverso i servizi da essi offerti (art. 4, par. 1), stabilisce specifici obblighi di *due diligence* in capo alle piattaforme al fine di promuovere «un ambiente online sicuro, prevedibile e affidabile» (art. 1, par. 1. In generale sul contrasto alla disinformazione nel DSA, cfr. E. LONGO, *Libertà di informazione e lotta alla disinformazione nel Digital Services Act*, in *Giornale di diritto amministrativo*, 2023, pp. 737-745; 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).

Non a caso, 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 processo elettorale (per un primo commento del caso, cfr. 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. 13/25, pp. 84-101; 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; J. ALBERT, *TikTok and the Romanian elections: A stress test for DSA enforcement*, in *DSA Observatory*, 20 December 2024). Da questo punto di vista, pertanto, la vicenda rumena offre l'occasione per riflettere sull'efficacia del DSA in materia di contrasto alla disinformazione *online*, in particolar modo allorché tale

fenomeno rischi di minare l'integrità dei procedimenti elettorali. Prima di approfondire le iniziative adottate in proposito dall'Unione europea, appare utile, al fine di delineare il contesto in cui ci si muove, ricostruire brevemente i fatti verificatisi in Romania.

2. *La sentenza di annullamento del primo turno delle elezioni presidenziali: la disinformazione come minaccia per lo stato di diritto*

All'indomani del voto, l'inaspettata vittoria al primo turno di Georgescu ha generato reazioni di forte stupore nell'opinione pubblica rumena, giacché, sulla base dei sondaggi diffusi alla vigilia, le sue possibilità di vittoria apparivano piuttosto esigue. Tale circostanza ha fatto sorgere il sospetto che un simile *exploit* fosse stato favorito dall'interferenza straniera di matrice russa, viste le note posizioni anti-NATO e anti-UE sostenute da Georgescu. In questo contesto, a seguito del ricorso presentato dalla candidata alla presidenza Cristian-Vasile Terhes in relazione a presunte irregolarità registratesi durante le procedure di voto, la Corte costituzionale ha ordinato il riconteggio delle schede ([sentenza n. 30 del 2024](#)). Non avendo riscontrato alcun errore, il 2 dicembre 2024 la Corte ha confermato l'esito del primo turno, autorizzando lo svolgimento del ballottaggio tra Georgescu e Lasconi ([sentenza n. 31/2024](#)).

Lo scenario, però, è mutato rapidamente, a seguito della diffusione, appena due giorni più tardi, di un *dossier* dei servizi di *intelligence* rumeni, precedentemente discusso in sede di Consiglio Supremo per la Difesa Nazionale. Tale documento segnalava come, nelle ultime settimane di campagna elettorale, sulla piattaforma TikTok si fosse registrata un'anomala campagna promozionale a sostegno di Georgescu, realizzata tramite inserzioni a pagamento, nonché condividendo contenuti politici sfruttando *account* fittizi creati *ad hoc* (oppure *account* esistenti ma sino ad allora inattivi).

A seguito di ciò, la Corte costituzionale è intervenuta *ex officio* per invalidare le elezioni, ritenendo che l'intero procedimento elettorale fosse stato viziato da gravi violazioni della legislazione vigente, suscettibili di pregiudicare taluni principi sanciti dalla Costituzione, quali il libero esercizio del diritto di voto e il principio delle pari opportunità dei candidati (per un commento della sentenza, cfr. 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). Affinché possano esprimere liberamente le proprie preferenze, infatti, è necessario che gli elettori siano in grado di formarsi un'opinione ricevendo informazioni puntuali sui candidati, senza essere influenzati in modo illecito o sproporzionato. Ebbene, secondo la Corte costituzionale, tale dinamica non si è concretizzata nel caso in esame, giacché la diffusione *online* di contenuti politici, di cui non era specificata né la matrice elettorale, né la sponsorizzazione da parte di attori stranieri, avrebbe avuto l'effetto di manipolare la volontà degli elettori, inducendoli in errore. L'esposizione digitale di Georgescu, amplificata dagli algoritmi di TikTok, avrebbe comportato, peraltro, la contestuale marginalizzazione nella rete degli altri candidati, di fatto impedendo una competizione realmente equa. Ricapitolando, dunque, la disinformazione ha operato in modo dissimulato, celando la natura politica dei contenuti pubblicati *online*, la cui diffusione è stata favorita dagli algoritmi della piattaforma attraverso inserzioni sponsorizzate da soggetti stranieri.

La sentenza è stata oggetto di numerosi commenti, ricevendo sia apprezzamenti per la capacità dimostrata dalla Corte di agire con vigore a tutela delle istituzioni e dei valori democratici, sia critiche per la limitatezza delle motivazioni avanzate sul piano giuridico,

nonché, sotto il profilo procedurale, per l'intervento *ex officio* anziché su istanza di parte, per le ristrette tempistiche con cui la procedura si è svolta e per il mancato coinvolgimento delle parti interessate (su questo dibattito, cfr. F. ROSA, *L'annullamento delle elezioni presidenziali in Romania e la difficile difesa della democrazia*, in [federalismi.it](https://www.federalismi.it), n. 15/2025, p. 62 ss.). Tralasciando tali aspetti, non rilevanti in questa sede, vale la pena sottolineare il fatto che la Corte costituzionale abbia basato la propria decisione sul presupposto che la disinformazione, erodendo uno dei capisaldi degli ordinamenti liberal-democratici, ossia la libertà di voto, possa costituire una strategia in grado di minare le fondamenta dello Stato di diritto (S. SASSI, A. STERPA, *La Corte costituzionale della Romania difende la democrazia liberale dalla disinformazione. Prime note sulla sentenza n. 32 del 6 dicembre 2024*, in [federalismi.it](https://www.federalismi.it), n. 4/2025, p. 163).

Per completezza di cronaca, si segnala che il primo turno delle elezioni presidenziali si è svolto il 4 maggio 2025. I due candidati più votati sono stati George Simion, anch'egli esponente di un partito sovranista (Alleanza per l'Unione dei Romeni), e l'indipendente Nicușor Dan, risultato vincitore al ballottaggio con il 53,60% delle preferenze. Georgescu non ha preso parte alla seconda tornata elettorale poiché la sua candidatura è stata respinta dall'ufficio elettorale, decisione poi confermata dalla Corte costituzionale, in quanto ritenuta, sulla scia dei fatti discussi in precedenza, non conforme ai valori costituzionali e ai principi cardine dell'ordinamento democratico, *in primis* lo svolgimento di elezioni eque e imparziali.

3. *Le disposizioni del DSA in materia di mitigazione dei rischi sistemici e le iniziative intraprese dalla Commissione a seguito delle elezioni in Romania*

Il caso rumeno ha evidenziato la facilità con cui le tecnologie digitali possano essere utilizzate per scopi manipolativi volti a destabilizzare le istituzioni democratiche. Nonostante sia ormai nota la vulnerabilità dei sistemi democratici nell'epoca plasmata dalle reti virtuali, l'intervento normativo in materia di contrasto alla disinformazione sconta talune criticità destinate a comprimere il raggio d'azione del legislatore. Innanzitutto, la nozione stessa di "disinformazione" è di difficile inquadramento, includendo non solo le notizie propriamente false, dunque teoricamente più facili da smascherare, ma anche quelle diffuse in modo fuorviante con l'intento di ingannare o manipolare l'utente, a prescindere dal loro contenuto (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). La mancanza di una definizione condivisa complica qualsiasi sforzo regolatorio, giacché ciascuna misura restrittiva, costituendo una limitazione della libertà di espressione, principio irrinunciabile per ogni ordinamento liberal-democratico, dovrebbe essere adottata con cautela: in caso contrario, si correrebbe il rischio di trasformare la lotta alla disinformazione in un potente strumento di controllo a disposizione dei governanti per soffocare arbitrariamente gli spazi democratici. La questione è resa ancor più scivolosa dal fatto che, nella prospettiva della Commissione, il concetto di disinformazione non si riferisca soltanto ai contenuti illegali e, quindi, rimuovibili in quanto tali, bensì assorba anche i contenuti formalmente leciti, ma comunque orientati ad arrecare un "pregiudizio pubblico", minacciando gli interessi fondamentali di uno Stato, nonché i valori costituzionali su cui esso si fonda (*ibidem*).

È questa la prospettiva adottata in proposito dal DSA, il cui art. 34, par. 1, impone ai fornitori delle piattaforme e dei motori di ricerca di dimensioni molto grandi – ossia, ai sensi dell'art. 33, gli operatori con un bacino medio mensile di destinatari del servizio nell'Unione almeno pari a 45 milioni – di individuare, analizzare e valutare con diligenza gli eventuali *rischi sistemici* «derivanti dalla progettazione o dal funzionamento del loro servizio e dei suoi relativi

sistemi, compresi i sistemi algoritmici, o dall'uso dei loro servizi»: ebbene, tali rischi sistemici includono non solo la diffusione di contenuti illegali oppure pregiudizievoli per l'esercizio dei diritti fondamentali, bensì anche gli «eventuali effetti negativi, attuali o prevedibili, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica» (lett. *c*). Ai sensi dell'art. 35, nel caso in cui le piattaforme e i motori di ricerca riscontrino, in qualsiasi aspetto del loro funzionamento, tali rischi sistemici, essi sono tenuti ad adottare «misure di attenuazione ragionevoli, proporzionate ed efficaci» (per un'analisi della nozione di “rischi sistemici” e delle sue implicazioni giuridiche, cfr. K. KAESLING, A. WOLF, *Sustainability and Risk Management under the Digital Services Act: A Touchstone for the Interpretation of 'Systemic Risks'*, in *GRUR International*, 2025, pp. 119-131). Tali misure possono riguardare l'adeguamento dei servizi forniti, delle condizioni generali, delle procedure di moderazione dei contenuti, dei sistemi algoritmici e di raccomandazione (per una panoramica di tali profili del DSA, cfr. L. D'AGOSTINO, *Disinformazione e obblighi di compliance degli operatori del mercato digitale alla luce del nuovo Digital Services Act*, in *MediaLaws*, n. 2/2023, p. 33 ss.).

La *ratio* di tale quadro normativo risiede nella convinzione che i *social network*, consentendo la rapida trasmissione dei contenuti a un numero potenzialmente enorme di utenti, possano essere utilizzati per «diffondere o amplificare contenuti fuorvianti o ingannevoli», suscettibili non solo di ledere i diritti fondamentali degli utenti, ma anche di produrre effetti negativi su questioni di interesse generale per la collettività, quali la salute pubblica, il pluralismo dei media e l'integrità delle consultazioni elettorali (DSA, considerando n. 84). Per tali ragioni, le piattaforme digitali sono chiamate in prima persona a rilevare i risvolti problematici dei loro servizi, adottando, se necessario, misure correttive: un onere senz'altro significativo, ma commisurato all'influenza esercitata dalle piattaforme digitali sul dibattito pubblico, in quanto volto ad escludere che quest'ultime possano offrire un megafono a chiunque intenda perseguire finalità discriminatorie, se non addirittura sovversive (E. BIRRIERI, *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*, n. 2/2023, p. 73).

Proprio l'eventuale violazione di tali disposizioni è al centro delle iniziative intraprese dalla Commissione europea nei confronti di TikTok in relazione alla vicenda rumena. Il 5 dicembre 2024, appena reso noto il rapporto dei servizi segreti rumeni che certificava l'interferenza della Russia nel procedimento elettorale, la Commissione ha emesso un “[ordine di conservazione](#)” nei confronti di TikTok, ordinando alla piattaforma di “congelare e conservare” i dati relativi ai rischi sistemici per i processi elettorali che potrebbero derivare dal suo servizio. Si tratta, in altre parole, di una misura preventiva, volta a preservare le informazioni utilizzabili in caso di avvio di un procedimento formale *ex art.* 66 del DSA nei riguardi di TikTok. L'ordine di conservazione, il cui ambito di applicazione temporale si estende al periodo compreso tra il 24 novembre 2024 e il 31 marzo 2025, riguarda la progettazione e il funzionamento dei sistemi di raccomandazione della piattaforma, nonché il modo in cui essa gestisce il rischio di manipolazione intenzionale attraverso un utilizzo illecito e coordinato del servizio. Tale misura si inquadra nei poteri di indagine conferiti dal DSA alla Commissione, i quali possono essere attivati su iniziativa di quest'ultima, come accaduto nel caso di specie, oppure su richiesta di un coordinatore nazionale dei servizi digitali (art. 65, par. 1). In effetti, sebbene il regolamento non menzioni esplicitamente l'emissione di un ordine di conservazione, la base giuridica di una misura di questo tipo può essere individuata nell'art. 67, il quale autorizza la Commissione, nell'esercizio delle sue

funzioni di controllo, a richiedere informazioni alla piattaforma (o al motore di ricerca) sotto osservazione a causa di una possibile violazione del DSA.

All'ordine di conservazione ha fatto seguito, due settimane più tardi, l'apertura di un procedimento formale nei confronti di TikTok *ex* articolo 66 del DSA. Secondo quanto si legge nel [comunicato](#) diffuso dalla Commissione, il procedimento è volto ad accertare l'eventuale violazione, da parte della piattaforma, degli obblighi ad essa incombenti ai sensi degli articoli 34, paragrafi 1 e 2, e 35, paragrafo 1, del DSA. Il sospetto della Commissione è che TikTok non abbia agito con la dovuta diligenza al fine di «valutare e attenuare adeguatamente i rischi sistemici legati all'integrità delle elezioni», in particolar modo per quanto riguarda i suoi sistemi di raccomandazione, nonché la sua *policy* in materia di pubblicità politica e contenuti politici a pagamento. Detto altrimenti, oltre a controllare il rispetto delle condizioni di servizio per quanto attiene alla diffusione di contenuti politici a pagamento, l'indagine intende esaminare le azioni intraprese dalla piattaforma allo scopo di mitigare gli effetti distorsivi che i suoi sistemi algoritmici potrebbero aver prodotto sull'andamento della consultazione elettorale.

L'avvio del procedimento segnala l'attenzione della Commissione nel proteggere il funzionamento dei sistemi democratici, evitando ingerenze indebite favorite dall'accessibilità della rete. Ciò detto, l'esito dell'indagine risulta difficilmente prevedibile. In effetti, come evidenziato altrove, la possibilità che emerga una “pistola fumante” in grado di accertare un collegamento diretto tra le attività disinformative *online* e i risultati delle elezioni appare un'ipotesi remota (S. WINDWEHR, *Systemic Risk Reporting: A System in Crisis?*, in [Electronic Frontier Foundation](#), 16 January 2025). L'impianto regolatorio stabilito dal DSA in materia di rischi sistemici è caratterizzato, infatti, da taluni limiti strutturali di cui occorre tenere conto.

Innanzitutto, il regolamento non stabilisce la soglia in base alla quale un rischio debba ritenersi *sistemico*, riservando alle piattaforme – nonché eventualmente al giudice, in caso di contenzioso – il compito di effettuare tale valutazione. In linea generale, appare ragionevole escludere che l'espressione possa riguardare episodi isolati, riferendosi semmai a un fenomeno sufficientemente strutturato da comportare una minaccia effettiva per l'interesse pubblico. Sebbene la pianificazione di una campagna disinformativa tesa ad interferire sul processo elettorale possa essere ricondotta piuttosto agevolmente al concetto di *rischio sistemico*, in altre circostanze tale associazione potrebbe risultare meno palese.

In secondo luogo, l'articolo 35 del DSA si limita ad elencare in termini generali le macro-tipologie delle misure di mitigazione che le piattaforme *possono* adottare, «ove opportuno», al fine di contrastare i rischi sistemici derivanti dai loro servizi, senza definire in concreto le modalità effettive di intervento. Tale impostazione è il risultato, presumibilmente, della difficoltà del legislatore di prevedere misure *standard* adatte a ciascuna piattaforma, dal momento che sia i servizi *online* esistenti, sia gli effetti dannosi che essi potrebbero determinare sugli interessi individuali e collettivi, si caratterizzano per un elevato livello di diversificazione (E. BIRRITTERI, *Contrasto alla disinformazione, Digital Services Act e attività di private enforcement*, cit., p. 75). Ne consegue, da un lato, che la portata di simili decisioni è rimessa *in toto* alla discrezionalità degli operatori privati (sul punto, cfr. N. ZINGALES, *The DSA as a Paradigm Shift for Online Intermediaries' Due Diligence*, in J. VAN HOBOKEN, 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.), dall'altro, che lo stesso potere di vigilanza esercitato dalla Commissione risulta depotenziato, non potendo fare affidamento su rigorosi *standard* di conformità stabiliti dal legislatore. Né tali criticità possono dirsi risolte dopo la pubblicazione, da parte della Commissione, delle [linee guida](#)

sulla mitigazione dei rischi sistemici per i processi elettorali, non solo perché, trattandosi di un atto di *soft law*, esse si limitano a fornire un ausilio ai gestori delle piattaforme sulle misure da integrare per affrontare i rischi individuati, ma anche perché tale documento reitera taluni limiti strutturali del DSA, come l'assenza di definizioni utili a chiarire la portata applicativa del regolamento, *in primis* in merito ai concetti di disinformazione e rischi sistemici (per un commento delle linee guida, cfr. N. PEUKERT, *Risky Recommendations. The European Commission Recommends Big Tech Measures to Mitigate "Systemic Risks" for Electoral Processes*, in [Verfassungsblog](#), 28 February 2024).

Siffatta elasticità, benché costituisca la spina dorsale del modello di "auto-regolamentazione forzata" istituito dal DSA, presuppone la capacità, nonché la disponibilità, delle piattaforme di plasmare gli interventi suggeriti dal regolamento sulla base delle specificità dei propri sistemi digitali (K. KAESLING, A. WOLF, *Sustainability and Risk Management under the Digital Services Act*, cit., p. 121). Questa circostanza espone l'impianto normativo a possibili cortocircuiti, come conferma la prima [relazione](#) presentata da TikTok ai sensi dell'articolo 42, paragrafo 4 del DSA, avente ad oggetto le valutazioni compiute dalla piattaforma in termini di rischi sistemici, nonché le relative misure di mitigazione adottate: ebbene, tra i profili critici individuati in materia di disinformazione elettorale, il documento non menziona l'azione non autentica coordinata, né la manipolazione dei sistemi di raccomandazione, proprio gli elementi al centro dell'indagine avviata dalla Commissione dopo le elezioni presidenziali in Romania. Tale episodio non stupisce: poiché i sistemi di raccomandazione costituiscono l'*asset* principale della strategia commerciale delle piattaforme, appare improbabile che i gestori di quest'ultime siano disposti a rivederne il funzionamento in termini sostanziali.

Quanto precede evidenzia la discrezionalità che il DSA concede alle piattaforme non solo nel determinare se, e in che misura, i loro servizi possano comportare rischi sistemici cui porre rimedio, ma soprattutto nel predisporre le strategie di mitigazione idonee a contrastare i pericoli individuati. Va da sé che anche la prospettiva sanzionatoria – la cui previsione costituisce, nelle intenzioni del legislatore, lo strumento principale per indurre le piattaforme ad allinearsi al dettato normativo – rischia di rivelarsi inefficace, potendo essere perseguita solo qualora la piattaforma abbia omesso del tutto o eseguito solo parzialmente l'attività di *risk assessment*, a prescindere dall'efficacia delle misure adottate (L. D'AGOSTINO, *Disinformazione e obblighi di compliance degli operatori del mercato digitale alla luce del nuovo Digital Services Act*, cit., p. 39). A meno che si materializzi lo scenario opposto, caratterizzato da un pronunciato attivismo della Commissione, la quale potrebbe sfruttare gli spazi vuoti del DSA per interpretare estensivamente le proprie funzioni di vigilanza, esercitandole ogniqualvolta il sistema democratico di un Paese membro appaia sotto pressione.

Da questo punto di vista, l'esito della vicenda TikTok nel caso rumeno costituirà un banco di prova utile a verificare l'efficacia del DSA nell'ottica di garantire il regolare svolgimento dei procedimenti elettorali negli Stati membri. Per il momento, [come riferito lo scorso 7 aprile dalla Commissaria per le tecnologie digitali Henna Virkkunen](#) di fronte alla commissione per il mercato interno e la protezione dei consumatori del Parlamento europeo, la Commissione europea ha «accolto con favore» le modifiche apportate da TikTok in materia di individuazione ed etichettatura degli account politici. Nessun cenno è stato fatto, invece, ai sistemi di raccomandazione utilizzati dalla piattaforma, sebbene anch'essi oggetto di contestazione da parte della Commissione. Nel frattempo, del resto, il risultato delle elezioni presidenziali di maggio ha stravolto il contesto politico. Ragion per cui la Commissione potrebbe decidere di chiudere il procedimento semplicemente prendendo atto degli impegni

assunti da TikTok *ex* articolo 71, paragrafo 1, del DSA allo scopo di correggere le criticità precedentemente individuate.

4. Conclusioni

A margine dell'analisi compiuta in queste pagine, appare utile svolgere talune considerazioni conclusive, seppur necessariamente parziali, poiché, al momento in cui si scrive, la Commissione non ha ancora annunciato la chiusura formale del procedimento nei confronti di TikTok. In ogni caso, al di là di eventuali sviluppi futuri, la vicenda esaminata offre l'occasione per tracciare un primo bilancio dell'efficacia del regime normativo definito dal DSA in materia di rischi sistemici.

Come si è cercato di far emergere, tale aspetto del DSA risulta permeato da un significativo grado di flessibilità, il quale interessa sia la portata degli obblighi di *due diligence* posti in capo alle piattaforme, sia l'incisività del relativo potere di controllo affidato alla Commissione. Il regolamento, infatti, riserva ai prestatori dei servizi di *hosting* il compito di stabilire quali misure correttive adottare al fine di risolvere le criticità individuate in fase di valutazione del rischio. Di conseguenza, non avendo a disposizione rigidi *standard* di conformità sanciti dal legislatore, la Commissione, nell'esercitare le proprie funzioni di vigilanza, beneficia di un apprezzabile margine di discrezionalità, il quale, a seconda delle contingenze politiche, può tradursi in una frequente attivazione del meccanismo sanzionatorio oppure, al contrario, in una sua tendenziale inutilità.

Uno schema normativo così concepito ci sembra coerente con la *ratio* di fondo del DSA, il quale, preme ricordarlo, si propone di armonizzare il funzionamento dei servizi di intermediazione digitale nell'ottica di proteggere diritti fondamentali e interessi comuni. Tale finalità presuppone una certa elasticità operativa da parte degli attori coinvolti, dal momento che, nello spazio digitale, ciascun intervento restrittivo comporta una compressione della libertà di espressione e informazione. La realizzazione in concreto di siffatto bilanciamento rappresenta la chiave di volta del DSA. Il regolamento ne affida l'esercizio agli *stakeholder* commerciali, i quali sono tenuti a contrastare gli effetti dannosi per la collettività derivanti dai loro servizi. Il potere decisorio riconosciuto alle piattaforme non è, però, privo di condizionamenti, giacché la rilevanza pubblica degli interessi in gioco rende necessario il coinvolgimento dei soggetti istituzionali a garanzia dell'ordine democratico. In tal senso, un ruolo decisivo è assegnato alla Commissione, tanto in ottica preventiva, attraverso l'elaborazione di linee guida e *best practices* volte ad assistere le piattaforme nel rispetto dei loro obblighi di *compliance*, quanto in chiave sanzionatoria, allorché l'approccio *soft* si riveli inadeguato ad arginare quei rischi sistemici suscettibili di minare le fondamenta stesse del processo d'integrazione europea.

Da questo punto di vista, la vicenda rumena ci restituisce una certezza: il tempo in cui le piattaforme potevano decidere in modo pressoché illimitato quali contenuti accogliere e quali rimuovere è definitivamente tramontato (cfr. A. GEESE, *Why the DSA could save us from the rise of authoritarian regimes*, in *Verfassungsblog*, 8 November 2022). La reattività dimostrata dalla Commissione nel caso di specie potrà costituire un deterrente per il futuro, favorendo una maggiore responsabilizzazione da parte dei gestori dei servizi digitali. Viene da chiedersi, tuttavia, se la disciplina prevista dal DSA consenta di proteggere efficacemente i sistemi democratici dai pericoli della rete, specialmente in presenza di strutturate campagne disinformative condotte da attori stranieri. La disinformazione si alimenta, infatti, attraverso i meccanismi algoritmici, i quali, intercettando gli utenti più sensibili a specifici contenuti,

hanno l'effetto di amplificare le notizie riportate in modo ingannevole, finendo per inquinare il dibattito pubblico. Ebbene, dal momento che tali sistemi costituiscono l'asse primario della strategia commerciale delle piattaforme, delegare a quest'ultime il compito di correggerne il funzionamento in via autonoma appare un'operazione sin troppo ottimistica. Sotto questo profilo, la sinergia tra l'auto-regolazione affidata ai *providers* e il *public enforcement* di matrice sovranazionale, elemento cardine del sistema di *governance* istituito dal DSA, rischia di rivelarsi inefficace, poiché esposta a interessi divergenti: rispettivamente, le esigenze economiche imposte dal mercato e la difesa dei valori fondamentali dell'Unione.

Ma c'è di più. Quanto discusso in questa sede risulta strettamente correlato agli eventi politici accaduti in Romania. Non ci si riferisce soltanto al *dossier* dei servizi di *intelligence*, ma soprattutto alla decisione della Corte costituzionale di annullare le elezioni per il sospetto di un'interferenza straniera capace di alterarne l'andamento: di fronte a una sentenza di tale portata, l'eventuale silenzio della Commissione sarebbe parso assai fragoroso. Qualora la strategia disinformativa non avesse raggiunto simili proporzioni, la Commissione avrebbe agito con analoga celerità? Certo, si può sostenere che in tal caso il rischio di un'ingerenza sul processo elettorale sarebbe stato meno pronunciato, quantomeno nell'immediato. L'erosione dei valori democratici, tuttavia, avviene spesso gradualmente: quando se ne manifestano gli effetti potrebbe essere già tardi per invertire la tendenza.

LORENZO DI ANSELMO