



## 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

### OSSERVATORIO NUOVE TECNOLOGIE E DIRITTI FONDAMENTALI

Coordinato da Francesco Battaglia

N. 1/2026  
15 marzo 2026



Co-funded by  
the European Union



### OSSERVATORIO NUOVE TECNOLOGIE E DIRITTI FONDAMENTALI N. 1/2026

#### 1. APPLICAZIONE ED *ENFORCEMENT* DEL *DIGITAL SERVICES ACT*. BREVI CONSIDERAZIONI SULLA SANZIONE DELLA COMMISSIONE EUROPEA A X

##### 1. *Introduzione: il caso X e l'applicazione del Digital Services Act*

Lo scorso 5 dicembre la Commissione europea ha comminato una multa di 120 milioni di euro a X, la piattaforma di proprietà di Elon Musk, per violazione del *Digital Services Act* (Regolamento 2022/2065 del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE, d'ora in avanti "DSA"). Si tratta della prima occasione in cui l'esecutivo dell'Unione ha adottato una decisione di non conformità ai sensi dell'art. 73 del DSA nei confronti di una *Very Large Online Platform* (VLOP; v. M. BOVERMANN, *The Limits of Symbolic Regulation*, in *Verfassungblog*, 18 dicembre 2025). Sebbene la Commissione abbia avviato anche altre indagini nell'ambito del DSA, nessuna di queste si è finora conclusa con un provvedimento di tale natura.

Il Regolamento 2022/2065 è la prima normativa sovranazionale a affrontare l'influenza delle piattaforme *online* sulla società, attraverso disposizioni volte a promuoverne la sicurezza, la trasparenza e la responsabilità nei confronti degli utenti (v. G. M. RUOTOLO, *Le proposte europee di riforma della responsabilità dei fornitori di servizi su Internet*, in *Rivista italiana di informatica e diritto*, 2022; C. CAUFFMAN, C. GOANTA, *A New Order: The Digital Services Act and Consumer Protection*, in *European Journal of Risk Regulation*, 2021, p. 758). Quanto agli obblighi previsti dal regolamento, esiste una differenza tra quelli che vincolano tutti gli intermediari, tra cui le piattaforme *online*, e, all'interno di queste ultime, quelli che sono indirizzati alle VLOPs, le quali, alla stregua dei VLOSEs (*Very Large Online Search Engines*) devono rispettare una serie di obblighi supplementari in materia di informazione e trasparenza e sono soggette a controlli più stringenti, alla luce dell'importanza che rivestono nel facilitare il dibattito pubblico, le operazioni economiche e la diffusione al pubblico di informazioni, opinioni e idee e nell'influenzare il modo in cui i destinatari ottengono e comunicano informazioni online (cfr. G. MORGESE, *Proposta di Digital Services Act e rimozione dei contenuti illegali online*, in P. MANZINI, G. CONTALDI, G. CAGGIANO (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, *Bari*, 2021, p. 47; A. Vicinanza, *La responsabilità delle piattaforme digitali nei confronti dei contenuti illegali: dal caso Telegram al Digital Services Act*, in *Quaderni AISDUE*, 2025). La Commissione ha il potere esclusivo di supervisione e di applicazione delle norme per quanto riguarda gli

obblighi relativi alle *VLOPs* e ai *VLOSEs*. A tal fine, la Commissione europea, ad aprile 2023, alla luce di quanto stabilito all'art. 33 DSA, ha designato diciannove società, di cui diciassette piattaforme e due motori di ricerca, come *VLOPs*, avendo un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni di utenti (v. F. BATTAGLIA, *Le prime sentenze sul Digital Services Act tra legittimità degli obblighi per le grandi piattaforme e limiti del sistema di designazione delle stesse*, in OIDU, 2025). Di conseguenza, al fine di verificare eventuali violazioni delle nuove norme, la Commissione ha inviato richieste di informazioni (*Requests for Information*, o *RFI*, art. 67 DSA) a diverse grandi piattaforme, tra cui *X Corp.* (ex *Twitter*), a partire da ottobre 2023. La *RFI* costituisce la prima fase di un'indagine ai sensi del *Digital Services Act*. A questa fase possono seguire ulteriori attività istruttorie, come l'accesso ai dati e agli algoritmi utilizzati dalla piattaforma, lo svolgimento di interviste con soggetti informati e ispezioni presso le sedi della piattaforma (artt. 68-69 DSA). Le informazioni raccolte tramite le *RFI* hanno portato all'avvio di diversi procedimenti per infrazione nei confronti delle varie piattaforme (art. 66 DSA). *X* è l'unica piattaforma il cui procedimento ha condotto all'adozione di conclusioni preliminari, annunciate dalla Commissione tramite un comunicato stampa. Inoltre, la decisione della Commissione europea di imporre una sanzione nei confronti di *X* rappresenta la prima tra i procedimenti avviati ai sensi del DSA a concludersi con un'ammenda.

Indipendentemente dal carattere innovativo, la decisione ha scatenato una dura reazione politica da parte di alcuni alti membri dell'amministrazione americana, che hanno definito per mezzo social l'esecutivo dell'Unione come "censore". A riprova del clima di tensione tra Unione europea e Stati Uniti riguardo al nuovo regime di obblighi e condotte dei colossi del *web*, il contenuto del provvedimento è stato reso pubblico alla fine di gennaio dall'*House Judiciary Committee Republicans*, la componente del Partito Repubblicano all'interno della Commissione Giustizia della Camera dei Rappresentanti degli Stati Uniti. La Commissione, infatti, non pubblica i documenti giuridici alla base delle proprie indagini nell'ambito del DSA e applica una presunzione generale di non divulgazione delle prove raccolte, comprese le richieste di informazioni. Ciononostante, il documento offre uno sguardo raro su come il *team* incaricato dell'applicazione del DSA costruisce i casi contro le grandi piattaforme e ci permette di esaminare le principali conclusioni della decisione relative a tre presunte violazioni contestate a *X* (ossia il *design* ingannevole delle spunte blu ai sensi dell'art. 25 del DSA), l'inaccessibilità del registro delle inserzioni pubblicitarie (ai sensi dell'art. 39) e le restrizioni all'accesso dei ricercatori ai dati pubblici (ai sensi dell'art. 40, par. 12).

## 2. *Violazione dell'articolo 25, par. 1 del Regolamento 2022/2065: la spunta blu e il fenomeno del dark pattern*

Come detto, l'obiettivo del DSA è di contribuire al corretto funzionamento del mercato interno dei servizi intermediari, stabilendo norme armonizzate per un ambiente *online* sicuro, prevedibile e affidabile (considerando 3 DSA; v. G. CAGGIANO, *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in I Post di AISDUE, 2021).

Muovendo da tali presupposti, il primo problema che emerge è che un numero crescente di persone ottiene le proprie notizie da fonti *online*, e tra queste fonti vi è anche *X*. Gli utenti della piattaforma consumano contenuti provenienti da una varietà di *account*, tra cui quelli di imprese commerciali, organizzazioni giornalistiche, enti governativi e politici (sul ruolo delle piattaforme online nel dibattito pubblico, v. A. VICINANZA, *Potere di opinione delle*

piattaforme digitali: come il *Digital Services Act* e il *Media Freedom Act* regolano la moderazione dei contenuti online, in C. SCHEPISI (a cura di), *Unione europea, pluralismo e libertà dei media nell'era digitale*, Napoli, Editoriale Scientifica, 2025; cfr. R. NEUVONEN, *Between Public and Private: Freedom of Speech and Platform Regulation in Europe*, in *European Public Law*, 2022). Considerato l'elevato numero di *account* presenti sulla piattaforma e il conseguente rischio di impersonificazione, *Twitter* aveva introdotto un sistema di verifica, comunemente noto come spunta blu (*blue badge* o *checkmark*; sul tema dell'impersonificazione, si veda K. ZAREI, R. FARAHBAKHSI, N. CRESPI, G. TYSON, *Impersonation on Social Media: A Deep Neural Approach to Identify Ingenuine Content*, in *IEEE/ACM ASONAM*, 2020). La spunta blu indicava che il personale di *Twitter* aveva verificato che l'*account* fosse effettivamente riconducibile alla persona o all'organizzazione in questione. Tale meccanismo ha contribuito a ridurre il rischio di impersonificazione e a rendere la piattaforma più trasparente e sicura per la ricezione delle informazioni. In un contesto in cui su una piattaforma *online* circola una notevole quantità di disinformazione, la spunta blu costituiva infatti uno strumento per identificare se le informazioni provenissero da una fonte legittima. Nel caso dei politici e delle organizzazioni governative, la principale preoccupazione era garantire che fosse chiaro se le informazioni provenissero effettivamente dal politico o dall'ente in questione e non da terzi. La spunta blu permetteva agli utenti di *Twitter*, inclusi i giornalisti, di riconoscere che un determinato *tweet* potesse essere considerato e citato come fonte legittima di informazione proveniente da quel politico (v. M. HAMAN, M. ŠKOLNÍK, *The unverified era: politicians' Twitter verification post-Musk acquisition*, in *Journal of Information Technology & Politics*, 2025). Dopo l'acquisizione di *Twitter* da parte di Elon Musk, sono state apportate numerose modifiche al funzionamento della piattaforma. Dall'aprile 2023, X ha iniziato a rimuovere la spunta blu dagli utenti che non avevano sottoscritto l'abbonamento *Twitter Blue* (l'attuale *X Premium*), che consentiva di ottenere la "verifica" e la spunta blu a pagamento. Di conseguenza, la spunta blu è scomparsa dagli *account* di molte personalità pubbliche che non erano disposte a pagare la quota mensile di 8 dollari richiesta per il servizio. Sono state coinvolte numerose agenzie governative, che hanno perso la spunta blu, con il possibile effetto di rendere meno trasparente per i cittadini l'identificazione delle informazioni provenienti da tali enti. Allo stesso tempo, è stato introdotto anche un nuovo contrassegno grigio per gli *account* verificati appartenenti a organizzazioni o funzionari governativi (oro per le *business organizations*).

*Twitter* è stato il pioniere del sistema di verifica degli *account* sui *social media* nel 2009, dopo aver constatato che la rimozione *ex post* dei contenuti impersonificati non era sufficiente a risolvere il problema degli *account* falsi. Negli anni successivi, le principali piattaforme di *social media* hanno generalmente seguito il modello di *Twitter*, offrendo sistemi di verifica degli *account* con terminologia e iconografia simili, basati sull'uso del simbolo della spunta blu (M. XIAO, M. WANG, A. KULSHRESTHA, J. MAYER, *Account Verification on Social Media: User Perceptions and Paid Enrollment*, in *Proceedings of the 32nd USENIX Security Symposium*, 2023). Lo scopo principale della verifica degli *account*, rimasto sostanzialmente costante nel tempo e tra le diverse piattaforme, con l'eccezione dei recenti cambiamenti introdotti su *Twitter*, è stato quello di contrastare l'impersonificazione degli *account* attraverso la conferma preventiva e proattiva dell'identità del titolare. Tuttavia, nel tempo la verifica ha acquisito anche altri significati, diventando non solo un indicatore di autenticità, ma anche un segnale di importanza dell'*account* e di credibilità dei contenuti pubblicati (sull'effetto degli indicatori di verifica sugli utenti, v. T. VAIDYA ET AL., *Does Being Verified Make You More Credible? Account Verification's Effect on Tweet Credibility*, *CHI Conference on Human Factors in Computing Systems*,

2019; S. EDGERLY, E. K. VRAGA, *The Blue Check of Credibility: Does Account Verification Matter When Evaluating News on Twitter?*, in *Cyberpsychology, Behavior, and Social Networking*, 2019).

La Commissione ha invece stabilito che «il fornitore di X si è discostato da un sistema di conferma dell'identità proattiva e preventiva (*ex ante*) verso un sistema nel quale lo *status* di “verificato” viene attribuito ad abbonati paganti anonimi, con un approccio almeno parzialmente reattivo e successivo (*ex post* ed *post hoc*) rispetto agli abusi di impersonificazione dello *status* di “verificato”» (punto 90 della decisione della Commissione, d'ora in avanti “decisione”).

In particolare, pur avendo la riforma di Musk sostituito il precedente sistema di verifica basato su un controllo approfondito dell'identità degli utenti con un meccanismo fondato principalmente sulla sottoscrizione di un abbonamento (*X Premium* e *Premium+*), la piattaforma ha mantenuto sostanzialmente invariato il *design* dell'interfaccia e il simbolo storico della spunta blu. La spunta blu è oggi principalmente associata alla sottoscrizione di un abbonamento a pagamento e non implica più necessariamente che l'identità dell'*account* sia stata verificata dalla piattaforma. Sulla base del sistema attuale, tale *status* indica soltanto che l'*account* dispone di un numero di telefono verificabile e di una carta di credito, e che non è stato individuato da X come intento di impersonare un'entità reale (punto 85). Orbene, lo stesso *provider* di X ha ammesso implicitamente che il processo iniziale di verifica, con cui si assegna la spunta blu, non è in grado di confermare con certezza l'identità o l'autenticità di un *account*, e questo perché la piattaforma consente e incoraggia gli utenti a segnalare eventuali *account* che violano la politica contro le impersonificazioni, mostrando che il sistema iniziale di verifica non è completamente affidabile (punto 81; sul ruolo degli utenti nel *fact-checking*, v. X HelpCenter, *About Community Notes on X*. Per un commento, cfr. M. MONTI, *La disinformazione online, la crisi del rapporto pubblico-esperti e il rischio della privatizzazione della censura nelle azioni dell'Unione Europea (Code of practice on disinformation)*, in *federalismi.it*, 2020).

Quanto ai criteri di idoneità per ricevere la spunta blu, nel precedente sistema di Twitter, un *account* doveva essere “attivo, noto e autentico”; i nuovi parametri di verifica sono invece “completo, attivo, sicuro e non ingannevole”, consentendo ad *account* anonimi o fittizi di ottenere la verifica. In linea di principio, nel precedente sistema di verifica, il requisito di autenticità presupponeva che l'*account* rappresentasse effettivamente la persona o l'entità indicata, con la conseguenza che gli *account* anonimi non potevano essere verificati. Nel sistema attuale, al contrario, il criterio di “non ingannevolezza” consentirebbe anche ad *account* anonimi o fittizi di ottenere la spunta blu, purché non violino le regole contro l'impersonificazione evidente (punto 84). Il *badge* ha tuttavia mantenuto lo stesso aspetto, quindi gli utenti possono erroneamente pensare che questi *account* siano stati verificati seriamente, ingannandoli sulla loro autenticità (punti 86 e 91). Secondo la Commissione, questa continuità visiva indurrebbe gli utenti a ritenere che gli *account* contrassegnati come “verificati” siano stati effettivamente sottoposti a un processo di verifica dell'identità analogo a quello in vigore nel il precedente sistema di *Twitter*. Tale discrepanza tra il significato storico della verifica e il funzionamento attuale del sistema è considerata dalla Commissione idonea a trarre in inganno gli utenti e a compromettere la loro capacità di valutare correttamente l'autenticità e l'affidabilità degli *account* presenti sulla piattaforma (punto 91).

La Commissione europea, a tal proposito, ha ritenuto che il nuovo sistema di verifica degli *account* introdotto da X non sia conforme all'art. 25, par. 1 del Regolamento (UE) 2022/2065, relativo ai cosiddetti *dark patterns*. Si tratta di tecniche di progettazione delle interfacce digitali che «indirizzano, ingannano, costringono o manipolano i consumatori inducendoli a compiere scelte che spesso non sono nel loro migliore interesse» (v.

Commissione europea, *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*, [Final Report](#), 2022, p. 20; v. anche European Data Protection Board, [Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them](#), 14 febbraio 2023). Tali tecniche, sulla base di studi di scienza cognitiva e di abitudini del comportamento umano, mirano a sfruttare i cc.dd. *bias* cognitivi degli utenti per l'esclusivo profitto dell'azienda che offre il servizio (v. A. SCAFFIDI, V. FORTE, *Dai Dark Patterns agli Hyper-Engaging Dark Patterns : per un'applicazione moderna del divieto ex art. 25 DSA*, in [mediaLaws](#), 2025; strettamente correlato è il concetto di *privacy* decisionale, per cui si rimanda a vedi G. DAY, A. STEMLER, *Are Dark Patterns Anticompetitive?*, in *Ala.L. Rev.*, 2020). Non esiste una [definizione](#) comune di *dark patterns* nel quadro giuridico dell'Unione. Il *Digital Services Act* le descrive nel considerando 67 come «pratiche che distorcono o compromettono in maniera significativa, sia intenzionalmente sia di fatto, la capacità dei destinatari del servizio di prendere decisioni o scelte autonome e informate», e che, come tali, sono vietate. Le varie [definizioni](#) condividono comunque due caratteristiche principali: la natura manipolatoria o ingannevole della pratica e il risultato negativo o dannoso che ne consegue.

A tal proposito, la Commissione ha evidenziato come la natura ingannevole dell'interfaccia di X sia ulteriormente rafforzata dal sistema di priorità algoritmica delle risposte (*reply prioritization*) riservato agli utenti abbonati ai servizi *X Premium* e *Premium+*. Tale funzionalità consente agli abbonati di ottenere una maggiore visibilità delle proprie risposte ai *post*, la quale aumenta con il livello dell'abbonamento. In questo modo, gli utenti possono di fatto “pagare per ottenere maggiore visibilità” dei propri contenuti (punto 92). Tuttavia, gli altri destinatari del servizio non vengono informati del fatto che tale maggiore esposizione dipende da un rapporto economico tra l'utente e la piattaforma. Secondo la Commissione, questo meccanismo, combinato con l'utilizzo della spunta blu, può indurre gli utenti a ritenere che i contenuti provenienti da *account* “verificati” siano più rilevanti o autorevoli, quando in realtà la loro maggiore visibilità deriva dal pagamento di un abbonamento. Di conseguenza, la piattaforma finisce per simulare artificialmente una forma di “notabilità”, compromettendo la capacità degli utenti di valutare in modo libero e informato la rilevanza e l'affidabilità dei contenuti visualizzati. La combinazione tra la percezione di autorevolezza associata alla spunta blu, la difficoltà degli utenti a reperire informazioni sul suo effettivo significato e la promozione algoritmica a pagamento degli *account* verificati ha portato la Commissione a concludere che tale funzionalità viola l'art. 25 DSA (punto 103).

### 3. *Violazione dell'articolo 39 del Regolamento 2022/2065: gli obblighi di trasparenza delle VLOPs sulle pubblicità online*

In secondo luogo, la Commissione ha rilevato la violazione dell'art. 39 relativo alla trasparenza pubblicitaria, ritenendo il *repository* pubblicitario di X non adeguatamente consultabile né affidabile, a causa di barriere di progettazione intenzionali (punto 287).

Le regole in materia di trasparenza svolgono un ruolo importante nel DSA, che, come in parte già anticipato, interviene in modo significativo su questi aspetti (v. P. Wolters, F. Z. Borgesius, *The EU Digital Services Act: what does it mean for online advertising and adtech?*, in [International Journal of Law and Information Technology](#), 2025). Più dettagliatamente, il DSA considera la pubblicità *online* un'attività intrinsecamente rischiosa (in tal senso si è pronunciato anche il Tribunale dell'Unione sul caso *Amazon EU Srl c. Commissione europea*, [causa T-367/23](#), del 19 novembre 2025, ECLI:EU:T:2025:1038, punto 89).

Il considerando 95 del DSA lo evidenzia esplicitamente, affermando che i sistemi pubblicitari «rappresentano rischi particolari e richiedono un'ulteriore supervisione pubblica e normativa a causa della loro portata e della capacità di indirizzare e raggiungere i destinatari del servizio in base al loro comportamento all'interno e al di fuori dell'interfaccia *online* della piattaforma o del motore di ricerca». Per questo motivo, il DSA richiede che le piattaforme *online* molto grandi, così come i grandi motori di ricerca creino archivi di annunci pubblicitari e li rendano disponibili nell'interfaccia utente, ricercabili tramite più criteri e accessibili tramite interfacce di programmazione applicativa (*Application Programming Interface*, o *API*). L'art. 39, par. 2 aggiunge ulteriori dettagli sulle informazioni che tale registro deve contenere. In particolare: *a*) il contenuto della pubblicità; *b*) la persona fisica o giuridica per conto della quale viene presentata la pubblicità; *c*) la persona fisica o giuridica che ha pagato la pubblicità, *d*) il periodo durante il quale è stata presentata la pubblicità; *e*) un'indicazione volta a precisare se la pubblicità sia destinata a essere presentata a uno o più gruppi specifici di destinatari del servizio e, in tal caso, i principali parametri utilizzati a tal fine, compresi, se del caso, i principali parametri utilizzati per escludere uno o più di tali particolari gruppi; *f*) le comunicazioni commerciali pubblicate sulle piattaforme; *g*) il numero totale di destinatari raggiunti.

Gli archivi sono stati creati con l'obiettivo di «facilitare la supervisione e la ricerca sui rischi emergenti derivanti dalla distribuzione della pubblicità online», con il considerando 95 che elenca esempi di «annunci illegali o tecniche manipolative e disinformazione con un impatto negativo reale e prevedibile sulla salute pubblica, sulla sicurezza pubblica, sul discorso civile, sulla partecipazione politica e sull'uguaglianza». Sempre sull'importanza della trasparenza della pubblicità online, anche il considerando 68 individua una serie di rischi significativi legati alla pubblicità online, tra cui la presenza di contenuti illegali, l'incentivazione di attività dannose o la discriminazione negli annunci. Ne consegue che la trasparenza non si configura come un obbligo meramente formale, bensì uno strumento essenziale di *due diligence* per identificare e mitigare tali rischi bensì (v. M. KNAPP, A. PISZCZ, «Moving Towards More Transparent Online Platforms Under the Digital Services Act», in D. V. POPOVIC, R. KULMS (a cura di), *Repositioning Platforms in Digital Market Law*, Springer, 2024) Quando questa viene meno, per esempio, perché le informazioni sugli annunci non sono facilmente accessibili, oppure non si può risalire a chi li finanzia o alle modalità di targetizzazione dei messaggi, si riduce la capacità degli utenti e delle autorità di valutare l'affidabilità e la legalità degli annunci, capire se determinati gruppi vengano discriminati o manipolati, individuare campagne pubblicitarie occulte che possono avere impatti sistemici sui processi democratici (v. G. PTRUZZELLA, *La libertà di informazione nell'era di Internet*, in *mediaLAW*, 2017). In altre parole, la trasparenza pubblicitaria è un presidio contro i rischi sistemici che le grandi piattaforme *online* possono contribuire ad alimentare nell'Unione (considerando 76 DSA).

In questo senso, nelle sue conclusioni preliminari sul caso X, la Commissione europea ha individuato una violazione dell'art. 39 del Regolamento (UE) 2022/2065, poiché il fornitore della piattaforma non avrebbe predisposto un archivio degli annunci pubblicitari conforme ai requisiti previsti da tale disposizione. In primo luogo, la Commissione ha ritenuto che lo strumento attraverso cui X ha reso disponibile il proprio archivio pubblicitario («*ads repository*») non costituisca uno strumento «consultabile e affidabile che consente ricerche attraverso molteplici criteri e attraverso le interfacce di programmazione delle applicazioni» (art. 39, par. 1 DSA). Per scaricare i dati sugli annunci pubblicitari su X, l'utente è tenuto a compilare tre campi obbligatori, ossia selezionare lo Stato membro in cui

L'annuncio è stato mostrato (senza la possibilità di includere tutti gli Stati dell'Unione), indicare l'account X dell'inserzionista tramite un menu a tendina e definire l'intervallo temporale di pubblicazione dell'annuncio. Poiché tutti e tre i campi devono essere compilati per ottenere un report, non è possibile effettuare ricerche basate su uno solo di tali criteri (punto 179). Secondo l'art. 39, par. 1 DSA, invece, lo strumento di ricerca dovrebbe consentire *query* multicriterio, comprendendo almeno tutte le informazioni previste dall'art. 39, par. 2 del Regolamento (punto 180). Inoltre, i risultati della ricerca non vengono mostrati direttamente in una sezione dell'interfaccia di X, come previsto dalla medesima disposizione, ma possono essere scaricati per poi essere visualizzati su *software* esterni, tipo *Excel*, il che rende il processo più complicato e meno immediato (punto 184).

In secondo luogo, l'archivio non fornisce informazioni su tutti gli annunci pubblicati su X fino a un anno dopo la loro ultima visualizzazione (criterio previsto dall'art. 39, par. 1). Se un inserzionista elimina un *post*, il contenuto diventa permanentemente non disponibile nel *repository*, in violazione dell'obbligo di conservare tali informazioni per un anno. Inoltre, lo strumento non mostra dettagli importanti, come il contenuto dell'annuncio, il prodotto o servizio pubblicizzati, il soggetto dell'annuncio, chi lo ha pagato o le comunicazioni commerciali pubblicate (punto 195). Altresì, i *report* generati contengono solo un *link* al post contenente l'annuncio pubblicitario, che può essere cancellato o modificato, rendendo impossibile rendendo impossibile, su larga scala e retroattivamente, recuperare le informazioni richieste (punto 204).

In terzo luogo, l'archivio pubblicitario di X non permette *query* tramite le interfacce di programmazione delle applicazioni, o *API*. L'utente è spesso costretto a ricorrere ad account autenticati e abbonati a piani *API* a pagamento, ma spesso risultano proibitivi e comunque tendenti all'errore, non fornendo alcun vantaggio reale rispetto allo strumento di ricerca gratuito (punti 202-212; v. L. EDELSON, G. INGE, F. LANCIERI, *Access to Data and Algorithms: For an Effective DMA and DSA Implementation*, CERRE, March 2023, p. 46 e ss.).

#### 4. *Violazione dell'art. 40, par. 12 DSA: garanzie di accesso ai dati per i ricercatori ai fini individuazione e prevenzione dei rischi sistemici*

Un ulteriore aspetto esaminato dalla Commissione nell'ambito del procedimento in esame è la conformità all'art. 40 DSA. Nell'ambito del suo sistema di gestione dei rischi, volto alla mitigazione dei cosiddetti rischi sistemici sulle piattaforme *online* di dimensioni molto grandi e sui motori di ricerca online di dimensioni molto grandi, il DSA introduce diritti di accesso ai dati per i ricercatori (v. M. NINO, *Researcher access to data from VLOPs and VLOSEs under the DSA*, in G. MORGESE, I. OTTAVIANO, S. PUGLIESE, N. RUCCIA (a cura di), *EU Rules on Transparency and Liability for Online Platforms. Challenges and Perspectives*, Torino, Giappichelli, 2025, p. 101). Attraverso questo strumento, il legislatore mira a consentire la produzione di evidenze relative a possibili minacce per la società e la democrazia che potrebbero essere collegate a tali piattaforme o motori di ricerca (v. A. LIESENFELD, *The Legal Significance of Independent Research based on Article 40 DSA for the Management of Systemic Risks in the Digital Services Act*, in *European Journal of Risk Regulation*, 2025).

Il legislatore ha distinto tra questi la figura dei ricercatori accreditati (*vetted researchers*). Per ottenere questo *status* da parte del coordinatore dei servizi digitali (autorità incaricata di vigilare sull'applicazione del regolamento e della sua esecuzione, considerando 110 e ss. DSA), i ricercatori devono soddisfare criteri piuttosto rigorosi. In primo luogo, devono essere affiliati a un'organizzazione qualificata come "organizzazione di ricerca" ai sensi della

direttiva sul diritto d'autore e sui diritti connessi nel mercato unico digitale (art. 2 della [direttiva 2019/790](#) del 17 aprile 2019, o direttiva DSM; v. art. 40, par. 8, lett. a) DSA), definizione che comprende università (incluse le loro biblioteche), istituti di ricerca o altre entità il cui obiettivo principale sia condurre ricerca scientifica o attività educative che includano la ricerca (v. M. NOVVIC, *The EU Digital Services Act (DSA). A commentary*, Alphen aan den Rijn, 2024, p. 293 e s.). Per essere considerata tale, l'organizzazione deve operare senza scopo di lucro oppure reinvestire tutti i profitti nella ricerca scientifica, oppure agire nell'ambito di una missione di interesse pubblico riconosciuta da uno Stato membro (considerando 97 DSA). Questo requisito è strettamente collegato alla seconda condizione prevista dal DSA, ossia l'indipendenza dei ricercatori accreditati dagli interessi commerciali (art. 40 par. 8 lett. b)). I candidati devono inoltre rendere pubbliche le fonti di finanziamento e garantire che i risultati della ricerca siano resi pubblicamente disponibili (art. 40, par. 8, lett. c) DSA). Questi requisiti si applicano cumulativamente a quelli previsti dalla direttiva 2019/790, la quale prevede che anche un ente finanziato con fondi pubblici potrebbe non soddisfare i criteri se il progetto di ricerca solleva dubbi sulla sua indipendenza o imparzialità (considerando 12 direttiva DSM; v. anche E. ROSATI, *Copyright in the Digital Single Market, Article-by-Article Commentary to the Provisions of Directive 2019/790*, Oxford, [2021](#)).

In secondo luogo, i ricercatori devono dimostrare di essere in grado di rispettare i requisiti di sicurezza, riservatezza e protezione dei dati, adottando adeguate misure tecniche e organizzative (art. 40, par. 8, lett. d) DSA). I ricercatori devono lavorare su un progetto chiaramente definito e rilevante. Lo *status* di ricercatore accreditato non è permanente, bensì l'accesso ai dati è concesso "unicamente" se la ricerca contribuisce alla comprensione o alla mitigazione dei rischi sistemici (ai sensi dell'art. 34, par. 1 DSA) e se i dati richiesti sono effettivamente "necessari" per lo specifico progetto (art. 40, par. 8, lett. e) DSA). I requisiti di necessità e di proporzionalità della richiesta d'accesso possono tuttavia risultare problematici, poiché nelle ricerche su fenomeni complessi non è sempre possibile definire con precisione i dati necessari prima di ottenere un accesso iniziale.

Infine, i ricercatori abilitati si impegnano a rendere gratuiti al pubblico i risultati delle ricerche condotte, in conformità al regolamento 2016/679 (Regolamento sulla protezione dei dati personali, [GDPR](#)). Una volta concesso lo *status*, il coordinatore dei servizi digitali presenta la richiesta motivata di accesso ai dati ai fornitori di piattaforme online a favore del ricercatore, o la revoca qualora non siano più soddisfatte le condizioni poc'anzi menzionate (art. 40, par. 4 e par. 10 DSA). Per fini di completezza espositiva, si segnala che ai sensi dell'art. 40, par. 13 DSA, la Commissione ha adottato recentemente il [Regolamento delegato 2025/2050](#), che ha stabilito le condizioni tecniche e armonizzato le procedure per la gestione del processo di accesso ai dati. Ha inoltre determinato quali informazioni i coordinatori dei servizi digitali, le piattaforme online di dimensioni molto grandi e i motori di ricerca online di dimensioni molto grandi devono rendere pubbliche per facilitare l'accesso dei ricercatori abilitati alle pertinenti serie di dati. Le domande dei ricercatori accreditati e le richieste di accesso ai dati ai sensi dell'articolo 40(4) del DSA saranno d'ora in avanti raccolte attraverso il nuovo portale dedicato [DSA Data Access Portal](#) (art. 3 Regolamento delegato 2025/2050).

Orbene, la figura del ricercatore accreditato appena descritta va distinta dal ricercatore indipendente, il quale non appartiene ad alcuna organizzazione o organismo senza scopo di lucro e si interfaccia direttamente con la piattaforma a cui sottopone la richiesta di accesso ai dati per le proprie ricerche, a cui è dedicato l'art. 40, par. 12 DSA. Ovviamente, si applicano anche ad essi le condizioni summenzionate (in particolare quelle alle lett. b), c), d) ed e)).

Dal punto di vista della conformità con l'art. 40, par. 12, il tentativo di monetizzazione del servizio di X con il cambio di proprietà ha eliminato l'accesso gratuito all'*API* di Twitter, che permetteva a soggetti esterni di monitorare su larga scala ciò che accadeva sulla piattaforma, e quindi anche ai ricercatori che studiano disinformazione e *hate speech*, a meno che non avessero pagato per continuare a utilizzare quei dati, e portando di conseguenza alla cessazione o cancellazione di diversi progetti di ricerca (punto 304).

In particolare, tra agosto e novembre 2023, X non ha predisposto alcun meccanismo dedicato per l'accesso ai dati da parte dei ricercatori, se non una costosa *API* (punto 301) e un indirizzo e-mail non pubblicizzato, che nel periodo di riferimento non è mai stato utilizzato per approvare alcuna richiesta (punto 309). La piattaforma consentiva anche un'*API* in versione gratuita con cui ottenere l'accesso ad un numero limitato di *post* al mese, cosa che ovviamente non permetteva ai ricercatori di raccogliere una quantità di dati sufficiente per fini di ricerca (punto 302).

Sebbene X abbia introdotto alcune misure volte a migliorare la gestione delle richieste di accesso ai dati da parte dei ricercatori accreditati, la Commissione ha ritenuto che tali interventi non siano stati sufficienti a garantire la conformità alle disposizioni del DSA. In primo luogo, X ha respinto alcune domande “sulla sola base del fatto che l'uso proposto dei dati di X da parte del richiedente non fosse esclusivamente destinato a ‘svolgere ricerche che contribuiscano all'individuazione, identificazione e comprensione dei rischi sistemici nell'UE come descritto dall'articolo 34’, nonostante tale requisito apparisse in realtà soddisfatto” (punto 319). Per la Commissione, si tratta di un'interpretazione inutilmente restrittiva della disposizione, ossia limitare l'accesso ai dati, sostenendo che una richiesta non sia sufficientemente specifica senza fornire ulteriori spiegazioni. La nozione di “esclusivamente” a cui fa riferimento l'art. 40, par. 12 del Regolamento (UE) 2022/2065 «non dovrebbe essere intesa come riferita all'ambito del progetto di ricerca o alla tipologia di dati ai quali deve essere concesso l'accesso, bensì alla finalità di tale accesso» (punto 321). La Commissione ha considerato che questa interpretazione sia ulteriormente supportata dal requisito secondo cui la ricerca deve “contribuire” a tale obiettivo, il che può essere realizzato attraverso un'ampia varietà di progetti di ricerca e mediante l'utilizzo di diversi campioni di dati. Così come limitativo risulta il rifiuto delle richieste di accesso ai dati da parte di ricercatori stabiliti in territorio extra-Ue, nonostante lavorino su progetti di ricerca dedicati all'identificazione e allo studio dei rischi sistemici nell'Unione (punto 325).

L'approccio restrittivo della piattaforma nel concedere l'accesso diretto dei ricercatori ai dati si è manifestato anche nella compilazione del [modulo](#) dedicato (che rientra, appunto, tra le nuove misure introdotte da X), che prevede campi obbligatori come l'affiliazione a organizzazioni o associazioni, requisito che invece l'art. 40, par. 12 del DSA non impone ai ricercatori indipendenti. Allo stesso modo, per soddisfare le condizioni dell'art. 40, par. 8, lett. b) e c), relative alla natura non lucrativa della ricerca e alla trasparenza dei finanziamenti, il provider di X richiede informazioni aggiuntive quali: (i) scopo e missione dell'organizzazione, (ii) dati sui membri del consiglio, sui dirigenti e sulle persone con accesso ai dati di X, (iii) ricerche precedentemente pubblicate, (iv) affiliazioni con altre organizzazioni, reti o cause, e (v) membri, azionisti o beneficiari di sovvenzioni. Si tratta di requisiti che eccedono quanto previsto dal Regolamento (UE) 2022/2065 e che risultano sproporzionati rispetto alla necessità di ottenere informazioni sul finanziamento della ricerca (punto 328).

La Commissione ha espresso, dunque, una valutazione preliminare secondo cui i processi adottati dal provider di X per esaminare le domande di accesso ai dati pubblicamente disponibili tramite l'*API* di X, ai sensi dell'art. 40, par. 12 del Regolamento (UE) 2022/2065,

nonché per comunicare agli interessati l'esito delle richieste, presentano carenze significative. Infatti, nonostante l'implementazione di un nuovo processo per concedere l'accesso ai ricercatori idonei tramite il modulo dedicato, nessuna richiesta è stata approvata prima del gennaio 2024 (punto 333), quando le disposizioni del DSA per le *VLOPs* erano già pienamente applicabili ad X dall'ottobre dell'anno precedente, quando era stata designata come piattaforma di grandi dimensioni (criterio dell'"accesso senza indebito ritardo ai dati"). I candidati ammessi, inoltre, verrebbero assegnati automaticamente al livello "Pro" dell'*API* di X (equivalente alla versione a pagamento da 5000 dollari), che consente per sei mesi l'accesso a un massimo di 1 milione di *tweet* al mese, una quantità dieci volte inferiore rispetto a quella prevista dal precedente programma di Twitter (punto 445; v. A. BRUNS, *After the 'APIcalypse': social media platforms and their fight against critical scholarly research*, in *Information, Communication & Society*, 2019). Nel frattempo, i termini di servizio di X continuano a vietare "tecniche di accesso indipendenti [...] come *scraping* e *crawling*", che sono "necessarie per svolgere ricerche sulla progettazione e sul funzionamento dei sistemi di raccomandazione di X" (punto 361; per una definizione v. B. MASSIMINO, *Accessing Online Data: Web-Crawling and Information-Scraping Techniques to Automate the Assembly of Research Data*, in *Journal of Business Logistics*, 2016; v. anche P. LEERSSEN, A. HELDT, M. C. KETTEMANN, *Scraping By? Europe's law and policy on social media research access*, in *Challenges and perspectives of hate speech research*, 2023, p. 405-425).

## 5. Conclusioni

Le violazioni degli articoli 25, 39 e 40, par. 12 sopra richiamate offrono un esempio del tipo di attività investigativa svolta in quasi tre anni di applicazione del DSA. Per costruire il proprio caso, la Commissione si è basata non solo sulle richieste di informazioni inviate a X ma anche su studi indipendenti, interviste con esperti e prove proprie, qualora le presunte violazioni fossero "auto-evidenti" (punto 566). L'avvio del procedimento segnala dunque l'attenzione della Commissione a proteggere gli utenti europei da pratiche ingannevoli, ma, in generale, a garantire il corretto funzionamento del sistema democratico nel suo insieme, evitando ingerenze indebite favorite dall'accessibilità della rete. L'aumento del costo di un *account* su X può essere efficace contro alcune forme di *spam*; tuttavia, tale misura rimane insufficiente per garantire l'autenticità sulla piattaforma, particolarmente vulnerabile ad attori indifferenti ai costi, come accade nei contesti elettorali. Per i governi nazionali coinvolti in campagne di manipolazione, un importo di 8 dollari è sicuramente trascurabile. Pertanto, questo non sembra costituire un deterrente significativo contro alcune delle forme di manipolazione più rilevanti dal punto di vista sociale (cfr. cfr. O. POLLICINO, P. DUNN, *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi (ed opportunità)*, in *federalismi.it*, n. 12/2024, p. iv ss.; 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.)

Proprio per questo, «[d]ata l'importanza che le piattaforme online di dimensioni molto grandi, per via del loro raggio d'azione, espresso in particolare come il numero di destinatari del servizio, rivestono nel facilitare il dibattito pubblico, le operazioni economiche e la diffusione al pubblico di informazioni, opinioni e idee e nell'influenzare il modo in cui i destinatari ottengono e comunicano informazioni online», il DSA ha imposto ai fornitori di tali piattaforme obblighi specifici, con cui individuano, analizzano e valutano con diligenza

gli eventuali rischi sistemici nell'Unione, e che solo un accurato sistema di verifica *ex ante* e *by design* può soddisfare (considerando 75 e art. 34 DSA).

Tale discorso si estende chiaramente anche ai rischi legati a una trasparenza carente nelle pubblicità online. Gli utenti della piattaforma consumano contenuti provenienti da una varietà di *account*, tra cui quelli di imprese commerciali, organizzazioni giornalistiche, enti governativi e politici. Nel caso dei politici e delle organizzazioni governative, la principale preoccupazione è garantire che le informazioni provengano effettivamente dal politico o dall'ente in questione e non da terzi. La spunta blu permetteva agli utenti di *Twitter*, inclusi i giornalisti, di riconoscere che un determinato *tweet* potesse essere considerato e citato come una fonte legittima di informazione proveniente da quel politico. Orbene, il caso rumeno e l'apertura di un procedimento formale nei confronti di *TikTok* hanno evidenziato la facilità con cui le tecnologie digitali possano essere utilizzate per scopi manipolativi volti a destabilizzare le istituzioni democratiche (v. 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 *OIDU*, 2025; M. COLI, *The Role of the European Union in Protecting Democracy through Legislation: The Case of Disinformation*, in *European Papers*, 2026). Allo stesso modo, il fenomeno del *microtargeting* politico ha acquisito un ruolo sempre più rilevante, grazie all'uso sofisticato delle tracce digitali lasciate dagli elettori. E le piattaforme *online* svolgono un ruolo cruciale in tal senso, consentendo la costruzione di campagne politiche mirate, capaci di identificare con precisione il pubblico di riferimento e di persuaderlo, adattando i messaggi alle caratteristiche specifiche di ciascun elettore (v. L. PIGNA, *Microtargeting politico nell'Unione europea. Alcune riflessioni alla luce della prassi istituzionale e della regolamentazione più recenti*, in *OIDU*, 2025). A questo punto, limitare l'accesso per i ricercatori, che contribuiscono all'individuazione, all'identificazione e alla comprensione di questi rischi sistemici, attraverso meccanismi restrittivi e dissuasivi, scoraggiando altri ricercatori dal presentare richiesta di accesso ai dati, influisce chiaramente sugli obiettivi del DSA. Occorre ricordare che le piattaforme non sono né possono essere neutrali nei confronti dei contenuti di terzi, proprio per il loro modello di profitto. Infatti, la durata dell'attenzione e il coinvolgimento degli utenti sono quantificabili come una risorsa economica che determina il profitto delle piattaforme. Per questo motivo, esse organizzano i *feed* e i risultati di ricerca in modo da mettere in evidenza contenuti capaci di attirare maggiore interesse, promuovendo temi di tendenza e raccomandazioni che spesso finiscono per privilegiare messaggi dal tono più sensazionalistico (v. 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, p. 45). Nel caso di X, tale effetto verrebbe ulteriormente amplificato dalla possibilità di ottenere uno status "verificato" tramite pagamento e da un sistema algoritmico che tende a privilegiare, nei risultati di ricerca e nella visibilità dei contenuti, gli account abbonati ai servizi a pagamento. Questo può disturbare o limitare la capacità degli utenti di valutare correttamente l'affidabilità e l'autenticità dei contenuti e degli *account*.

A margine dell'analisi compiuta in queste pagine, le brevi osservazioni conclusive svolte sono necessariamente parziali, poiché non solo la Commissione deve ancora spiegare le scelte giuridiche a supporto della segretezza del suo processo di applicazione, in seguito alla divulgazione inattesa della decisione su X, ma soprattutto perché al momento in cui si scrive, i *provider* di X nell'Unione europea, vale a dire *X Internet Unlimited Company* (XIUC), *X Holdings Corp.*, *X.AI Holdings Corp.*, e Elon Musk, hanno presentato ricorso avverso al provvedimento della Commissione che, a quanto dicono i ricorrenti, è il risultato di

un'indagine incompleta e superficiale, viziata da gravi errori procedurali e da un'interpretazione forzata degli obblighi previsti dal Digital Services Act.

Il caso rappresenta dunque il primo ricorso di una sanzione inflitta ai sensi del DSA davanti al giudice dell'Unione e potrebbe stabilire importanti precedenti in materia di applicazione della normativa, di determinazione delle sanzioni e di tutela dei diritti fondamentali nell'ambito del DSA.

LUIGI PIGNA