



La guerra invisibile contro le democrazie: l'AI moltiplica le interferenze, l'Italia rischia di arrivare impreparata

Descrizione

(Adnkronos) L'Europa ha imparato a riconoscere molte delle operazioni con cui attori stranieri cercano di manipolare il dibattito pubblico, alimentare la polarizzazione e condizionare le elezioni. Conosce le reti, le tecniche utilizzate e, in diversi casi, anche le strutture che coordinano queste campagne. Eppure continua a incontrare enormi difficoltà nel fermarle. Nel frattempo, l'intelligenza artificiale rende più semplice produrre contenuti falsi credibili, moltiplicarne la diffusione e adattarli alle fragilità politiche e sociali di ciascun Paese.

È questo il paradosso emerso dal confronto europeo sulla disinformazione che si è tenuto a Roma, all'Europa Experience David Sassoli con rappresentanti delle istituzioni europee, del Parlamento italiano, delle ambasciate accreditate in Italia e delle principali organizzazioni impegnate nel contrasto alle interferenze informative straniere.

Sul tavolo, una domanda che riguarda direttamente anche l'Italia, attesa dalle elezioni politiche del 2027: come si difende l'integrità di un processo democratico quando la manipolazione dell'informazione non si limita alla campagna elettorale, ma opera in modo permanente, attraverso infrastrutture digitali transnazionali e con strumenti sempre più sofisticati?

La dimensione del fenomeno emerge dai dati del Servizio europeo per l'azione esterna (Seae), richiamati nel rapporto finale del progetto FIMI Defenders for Election Integrity (FDEI). Nel 2025 sono stati documentati e analizzati 540 episodi di manipolazione e interferenza informativa straniera, conosciuta con l'acronimo FIMI, che hanno coinvolto circa 10.500 canali e 43mila contenuti. Il 29% degli episodi è stato attribuito alla Russia e il 6% alla Cina. Il restante 65% non ha ricevuto un'attribuzione statale certa, pur presentando in diversi casi indicatori di coordinamento con infrastrutture russe o cinesi.

Particolarmente significativo il ruolo dell'intelligenza artificiale: le tecniche basate sull'AI sono state rilevate nel 27% degli episodi, passando da 41 casi nel 2024 a 147 nel 2025. Una trasformazione delle modalità con cui possono essere esercitate pressioni sulle democrazie europee.

L'evento, intitolato *Securing Democratic Discourse: Election Integrity in an AI-Disinformation Era*, ha presentato i risultati del progetto FDEI, una collaborazione tra dieci organizzazioni europee e internazionali impegnate nel monitoraggio e nel contrasto alla manipolazione dell'informazione nei processi elettorali.

L'evento è stato ospitato dall'Ufficio del Parlamento europeo in Italia e organizzato dal DEN Institute e da Debunk.org per conto del consorzio FDEI, sviluppato nell'ambito del FIMI Information Sharing and Analysis Centre (FIMI-ISAC).

50 partecipanti, tra i quali 19 rappresentanti di 13 missioni diplomatiche accreditate a Roma, si sono confrontati con esponenti della Commissione europea, del Servizio europeo per l'azione esterna, del Parlamento europeo e del Senato italiano.

Tra le istituzioni rappresentate figuravano la Direzione generale Comunicazione della Commissione europea, il Servizio europeo per l'azione esterna attraverso le strutture responsabili dell'integrità dell'informazione, e il ministero degli Affari esteri e della Cooperazione internazionale, attraverso l'unità dedicata alle minacce ibride. Al confronto hanno contribuito organizzazioni specializzate come GLOBSEC, Institute for Strategic Dialogue (ISD), EU DisinfoLab, Digital Forensic Research Lab dell'Atlantic Council, NASK, CEE Digital Democracy Watch, Context.ro e Fundaci3n Maldita.es.

Dal confronto è emerso un nodo fondamentale: gli strumenti per individuare le campagne di interferenza esistono, ma manca ancora un sistema sufficientemente integrato e rapido per trasformare le segnalazioni in risposte concrete. Le dichiarazioni raccolte dall'Adnkronos a margine dell'incontro aiutano a comprendere la portata della sfida.

Per Marco Lombardo, senatore di Azione, la disinformazione e le interferenze straniere non sono più un tema specialistico, da lasciare esclusivamente agli apparati di sicurezza.

La più grave minaccia che oggi abbiamo per la sicurezza nazionale ed europea, afferma ad Adnkronos. Incontri come quello di oggi mostrano che c'è una grande consapevolezza tra accademici, istituzioni e mondo delle ambasciate. Il problema è che non può rimanere solo una cosa per addetti ai lavori. Deve arrivare davvero al dibattito pubblico e farci capire quanto dobbiamo essere mobilitati in difesa dell'integrità dei processi democratici elettorali, perché le nostre democrazie sono minacciate dalla guerra ibrida.

Se la manipolazione dell'informazione è parte integrante delle strategie di guerra ibrida, il suo contrasto non può essere affidato soltanto ai servizi di intelligence e alle autorità di sicurezza. Deve diventare una questione politica condivisa.

Credo che questo tipo di operazioni debbano uscire dall'ambito di pertinenza del Copasir o dei servizi, insiste Lombardo, chiedendo che diventino parte integrante del confronto pubblico.

Il problema, secondo il senatore, è che in Italia manca ancora la disponibilità politica ad affrontare il tema in modo trasversale. Lombardo ricorda che, insieme a Carlo Calenda, ha presentato nell'aprile 2025 due iniziative legislative per la difesa delle libertà costituzionali e dell'integrità del processo democratico dalle ingerenze straniere. Si tratta del disegno di legge ordinario 1473, dedicato all'istituzione di uno scudo democratico, e del disegno di legge costituzionale 1472, sulla tutela del processo elettorale. Entrambi sono stati assegnati alla commissione Affari costituzionali del Senato nel

maggio 2025, senza che ne sia ancora iniziato l'esame.

«In Italia questo tema rischia di far esplodere le contraddizioni nelle coalizioni, per cui non se ne parla», osserva Lombardo, richiamando il dibattito francese sulla necessità di un impegno condiviso contro le ingerenze straniere. «Occorre il coraggio di avere davvero la consapevolezza di quanto oggi siamo il ventre molle, per esempio, delle ingerenze russe».

I risultati del progetto FDEI aiutano a comprendere perché individuare una campagna di interferenza non equivalga a neutralizzarla.

Tra le operazioni analizzate figurano Doppelganger, Storm-1516, Operation Overload e la rete Pravda, conosciuta anche come Portal Kombat. Non si tratta di singole notizie false pubblicate sui social network, ma di sistemi organizzati e persistenti, capaci di produrre, ripubblicare e amplificare contenuti attraverso reti di siti internet, account e piattaforme differenti.

L'obiettivo non è necessariamente convincere un elettore attraverso un messaggio isolato, ma creare un ambiente informativo nel quale una determinata narrazione viene ripetuta da molteplici fonti apparentemente indipendenti, fino a diventare familiare e credibile.

Emblematico il caso della rete Pravda, identificata dall'agenzia francese VIGINUM come Portal Kombat. Il sistema aggrega contenuti filorussi attraverso oltre duecento sottodomini legati a Paesi e lingue differenti. Tra il primo settembre e il 9 ottobre 2025, il solo sottodominio in lingua ceca ha ripubblicato più di 200mila contenuti, 822 dei quali specificamente legati alle elezioni.

L'enorme quantità di materiale serve anche a far sì che i contenuti possano essere indicizzati dai motori di ricerca, ripresi da altri siti e successivamente rilanciati, perdendo progressivamente la riconoscibilità della propria origine.

La disinformazione contemporanea non cerca soltanto di diffondere messaggi falsi: cerca di costruire l'apparenza di un ecosistema informativo attendibile. Una caratteristica che rende estremamente difficile combatterla intervenendo soltanto sui singoli contenuti.

Il progetto FDEI ha monitorato le elezioni del 2025 in Germania, Polonia, Moldavia e Repubblica Ceca, applicando metodologie comuni per rendere confrontabili episodi e comportamenti delle piattaforme.

In Germania sono state documentate campagne riconducibili a operazioni già individuate negli anni precedenti. Doppelganger ha continuato a diffondere contenuti attraverso siti e profili che imitavano fonti credibili. Operation Overload ha utilizzato sistemi di amplificazione coordinata, mentre Storm-1516 ha fatto ricorso a oltre cento siti che pubblicavano contenuti generati con l'AI nei tre mesi precedenti al voto.

Le visualizzazioni osservate sono state stimate complessivamente intorno ai 55 milioni, un dato che tuttavia non dimostra un'influenza equivalente sull'opinione pubblica, anche a causa dell'amplificazione artificiale.

Il problema più significativo ha riguardato la risposta delle piattaforme. Secondo il rapporto FDEI, i contenuti riconducibili a Storm-1516 sono stati segnalati anche attraverso i meccanismi previsti dal Digital Services Act. X ha respinto le segnalazioni sostenendo che i contenuti non fossero illegali,

mentre Bluesky Ã intervenuta sugli stessi materiali, registrando successivamente un forte calo dell'attivitÃ collegata alla campagna.

In Polonia, durante le presidenziali, sono stati individuati circa seicento contenuti riconducibili a Doppelganger tra aprile e maggio 2025. Le rimozioni di centinaia di account non hanno impedito la prosecuzione dell'operazione. Il monitoraggio ha inoltre documentato una campagna pubblicitaria su Meta con una spesa di circa 100mila euro per raggiungere un milione di utenti.

Ancora piÃ¹ complesso il caso della Moldova, uno dei Paesi maggiormente esposti alle interferenze russe. Il rapporto descrive una strategia decentralizzata basata su falsi organi di informazione, siti clonati, reti di influencer retribuiti, contenuti generati con l'AI e tentativi di compromettere la fiducia nel processo elettorale.

Particolare attenzione Ã stata riservata alla diaspora moldava, bersaglio di campagne volte a condizionarne o scoraggiarne la partecipazione al voto. Le autoritÃ hanno anche chiesto il blocco di 443 canali TikTok che raccoglievano complessivamente oltre 1,2 milioni di follower. Secondo quanto successivamente dichiarato dal vertice della polizia nazionale, circa il 95% dei contenuti segnalati non sarebbe stato rimosso, sebbene il rapporto precisi di non aver potuto verificare autonomamente tutte le richieste.

La Repubblica Ceca offre invece un elemento di cautela. Nonostante la presenza di una rete TikTok di 146 account coordinati e la massiccia attivitÃ di Portal Kombat, il monitoraggio non ha individuato un'operazione coordinata della quale fosse possibile dimostrare la capacitÃ di influenzare il risultato elettorale.

La crescente capacitÃ delle campagne straniere di adattarsi ai contesti nazionali Ã al centro del lavoro dell'Institute for Strategic Dialogue, organizzazione internazionale che studia estremismo, polarizzazione e manipolazione dell'informazione.

Melanie Smith, senior director di ISD, racconta ad Adnkronos come queste operazioni stiano cambiando forma. (VIDEO)

Abbiamo osservato campagne condotte da attori allineati alla Russia, in particolare nelle recenti elezioni regionali tedesche. Sono molto simili a quelle che abbiamo visto nelle elezioni nazionali del 2024 e del 2025, ma stanno diventando piÃ¹ locali e piÃ¹ adattate ai singoli contesti politici. Si tratta soprattutto di video che impersonano personaggi pubblici, talvolta candidati alle elezioni o giornalisti. Sembrano autentici, ma utilizzano voci generate con l'intelligenza artificiale per far apparire quelle persone come se stessero dicendo cose che in realtÃ non hanno mai detto.

Il problema non Ã soltanto individuare questi contenuti, ma far circolare le informazioni tra ricercatori, autoritÃ pubbliche e piattaforme.

Le infrastrutture e i meccanismi esistono, ma non sono molto ben coordinati, spiega Smith. Abbiamo molti di questi strumenti e sappiamo cosa bisognerebbe fare, ma metterlo in pratica Ã ancora piuttosto difficile. Per ricercatori come noi Ã molto difficile capire cosa i governi sappiano e cosa non sappiano di quello che accade durante le elezioni, perchÃ© lo scambio di informazioni di intelligence Ã molto limitato. Spesso siamo noi a segnalare preventivamente le attivitÃ alle autoritÃ, ma non ci Ã chiaro come rispondano, se rispondano e se gli obiettivi vengano effettivamente

raggiuntiâ?•.

Per Smith, la persistenza di operazioni come Doppelganger dimostra i limiti di un contrasto basato esclusivamente sulla rimozione degli account.

â??Siamo ancora nella situazione di dover rincorrere continuamente queste operazioniâ?•, osserva, utilizzando lâ??espressione inglese whack-a-mole, il gioco nel quale si tenta di colpire talpe che continuano a riapparire. â??Riusciamo a far rimuovere alcuni account e speriamo che sia efficace. Ma, alla fine, il successo di queste campagne dipende dal fatto che vengano riprese dai pubblici nazionali e dalle voci interne ai singoli Paesiâ?•.

Lâ??ingerenza straniera diventa particolarmente efficace quando non ha piÃ¹ bisogno di apparire straniera. Una narrazione fabbricata allâ??estero puÃ² essere ripresa da influencer, siti di informazione, comunitÃ digitali e soggetti politici nazionali, fino a inserirsi nel dibattito pubblico come una posizione apparentemente spontanea.

â??Ã? importante continuare a rimuovere queste attivitÃ quando le individuiamo, ma serve una risposta piÃ¹ complessivaâ?•, prosegue Smith. â??Le persone devono capire che cosa sia la manipolazione dellâ??informazione e come riconoscere i contenuti prodotti dallâ??AIâ?•.

Lâ??esperta insiste soprattutto sulla preparazione dei cittadini prima delle elezioni: spiegare in anticipo che potrebbero essere bersaglio di campagne manipolative, mostrare come riconoscerle e chiarire quali segnali osservare nei propri flussi informativi. â??Purtroppo, questo non sta ancora avvenendo in modo coordinato e su larga scalaâ?•.

La vulnerabilitÃ delle democrazie europee non dipende soltanto dalla sofisticazione tecnologica degli strumenti di disinformazione. Ã? strettamente collegata alla fiducia che i cittadini ripongono nelle istituzioni.

Katarina Klingova, del Centro per la democrazia e la resilienza di GLOBSEC, osserva il fenomeno da un punto di vista particolarmente significativo: quello dellâ??Europa centrale e orientale.

â??Abbiamo osservato che in diversi Paesi una parte molto ampia della societÃ crede a queste narrazioni perchÃ© non ha fiducia nelle istituzioni pubblicheâ?•, spiega ad Adnkronos. (VIDEO)

Klingova richiama le ricerche di GLOBSEC sulle tendenze dellâ??opinione pubblica, condotte attraverso rilevazioni periodiche dal 2016.

â??In alcuni Paesi, come Bulgaria, Slovacchia e Romania, da un terzo fino al 40% della popolazione mostra vulnerabilitÃ a diverse narrazioni polarizzanti, con una profonda sfiducia nelle istituzioni. Queste narrazioni distruggono non soltanto la coesione sociale, ma anche la fiducia nei processi democratici e nelle elezioniâ?•. La disinformazione non opera nel vuoto: trova terreno fertile dove esistono fratture sociali profonde, sfiducia nei partiti, risentimento verso le istituzioni. Le operazioni straniere possono sfruttare queste fragilitÃ , amplificandole e orientandole.

Klingova ricorda come, dopo lâ??annessione russa della Crimea nel 2014, in Europa centrale alcuni siti abbiano radicalmente cambiato la propria linea editoriale, passando persino da contenuti sportivi alla diffusione di propaganda politica.

Oggi la sfida Ã ulteriormente complicata dall'uso dell'intelligenza artificiale e dalla capacitÃ degli attori ostili di reagire piÃ¹ rapidamente delle istituzioni democratiche. âCon lo sviluppo dell'AI e dei nuovi strumenti di comunicazione non possiamo permetterci di rilassarciâ, afferma. âÃ una battaglia che non finisce mai. Non si costruisce la resilienza democratica di uno Stato membro o dell'Unione europea da un giorno all'altro. Ã un processo di lungo periodo che coinvolge tutto il governo e tutta la societÃ â. Alla domanda se l'Europa sia pronta al prossimo ciclo elettorale, la risposta Ã prudente. âNon saremo mai pronti al 100%, a causa della rapiditÃ con cui cambiano le tecnologie utilizzate dai nostri avversariâ.

Per Klingova esiste una differenza strutturale tra il funzionamento delle democrazie e quello dei regimi autoritari: le prime devono discutere, cercare compromessi e costruire decisioni condivise; i secondi possono agire rapidamente, senza gli stessi vincoli istituzionali. âDobbiamo reagire piÃ¹ velocemente, scambiare informazioni piÃ¹ rapidamente e coinvolgere tutti gli attori allo stesso tavolo: istituzioni pubbliche, societÃ civile, ma anche imprese private. PerchÃ© anche queste ultime hanno un ruolo enorme nella protezione della resilienza democraticaâ.

La risposta istituzionale europea si sta sviluppando attorno all'European Democracy Shield, lo scudo europeo per la democrazia, presentato dalla Commissione nel novembre 2025. L'iniziativa punta a rafforzare l'integritÃ dello spazio informativo, la protezione delle elezioni, l'indipendenza dei media e la capacitÃ della societÃ civile di resistere alla manipolazione e alle interferenze straniere.

Uno degli strumenti principali Ã il Centro europeo per la resilienza democratica, che ha avviato le proprie attivitÃ nel febbraio 2026. Il Centro mette in collegamento istituzioni europee e Stati membri, tra cui l'Italia, con l'obiettivo di migliorare l'individuazione delle minacce, la condivisione delle informazioni e la capacitÃ di risposta coordinata.

Il problema Ã trasformare questa architettura in una capacitÃ realmente operativa. L'esperienza delle campagne analizzate dal progetto FDEI indica che non basta aggiungere nuove strutture a quelle giÃ esistenti. Occorre stabilire chi sia responsabile di ricevere una segnalazione, verificarne il contenuto, trasmetterla alle autoritÃ competenti e assicurare che venga presa in considerazione.

Lo stesso Digital Services Act, che offre un quadro regolatorio per affrontare i rischi sistemici delle grandi piattaforme digitali, deve confrontarsi con la difficoltÃ di accedere tempestivamente ai dati e verificare l'efficacia delle misure adottate.

Il punto riguarda anche la distinzione tra disinformazione e libertÃ di espressione. Un'opinione controversa, una critica politica o una notizia inesatta non possono essere automaticamente assimilate a un'operazione di interferenza straniera. Per questo la risposta deve basarsi su comportamenti coordinati, infrastrutture, prove documentabili e trasparenza dei finanziamenti, evitando di trasformare la difesa del pluralismo in uno strumento di controllo delle opinioni.

Uno dei risultati piÃ¹ importanti del progetto FDEI Ã la costruzione di una metodologia comune per monitorare le interferenze informative.

Il consorzio ha prodotto quattro valutazioni preventive dei rischi elettorali e quattro rapporti successivi alle elezioni, 117 segnalazioni strutturate di incidenti, una base di oltre 500 casi prioritari codificati e programmi di formazione che hanno coinvolto piÃ¹ di cento analisti.

Le organizzazioni partecipanti hanno utilizzato classificazioni condivise per registrare tattiche, tecniche, procedure, infrastrutture e narrazioni. L'obiettivo è rendere le informazioni raccolte in un Paese confrontabili e utilizzabili anche da ricercatori e istituzioni di altri Stati.

Una differenza sostanziale rispetto a un sistema nel quale ogni organizzazione conduce autonomamente le proprie indagini e deve ricostruire da zero i rapporti con le autorità ogni volta che si presenta una crisi.

Il rapporto conclusivo del progetto individua tuttavia due interrogativi ancora irrisolti: chi debba assumersi la responsabilità di colmare i vuoti operativi e come garantire finanziamenti continuativi alle organizzazioni che producono gran parte delle informazioni utilizzate dalle istituzioni.

Il progetto FDEI ha infatti una scadenza fissata a gennaio 2027. Senza un sistema stabile di collaborazione e sostegno, una parte delle competenze e delle reti sviluppate negli ultimi due anni rischia di andare dispersa proprio mentre l'Europa si avvicina a un nuovo ciclo elettorale.

Le elezioni che attendono diversi Paesi europei nel 2027 costituiscono un banco di prova per il nuovo sistema di difesa democratica. Francia e Italia, in particolare, saranno chiamate ad affrontare campagne politiche potenzialmente esposte a operazioni di manipolazione, amplificazione artificiale e interferenze straniere.

Non significa che queste operazioni siano destinate ad alterare i risultati elettorali. La stessa esperienza del progetto FDEI dimostra quanto sia difficile stabilire un rapporto causale tra campagne di disinformazione e comportamento degli elettori.

Il problema riguarda piuttosto la capacità di proteggere le condizioni nelle quali il confronto democratico si svolge: accesso a informazioni verificabili, trasparenza delle campagne digitali, riconoscibilità delle fonti, pluralismo e fiducia nell'integrità del voto.

Per l'Italia questa sfida presenta due dimensioni. La prima è istituzionale: rafforzare la capacità di coordinamento tra autorità nazionali, istituzioni europee, piattaforme e ricercatori indipendenti. La seconda è politica: riconoscere la minaccia in modo trasversale, senza trasformare ogni iniziativa di contrasto in una nuova occasione di scontro tra maggioranza e opposizione.

La sfida non è semplicemente eliminare le notizie false, obiettivo di per sé irrealistico. È fare in modo che le democrazie sappiano riconoscere e contrastare le operazioni sistematiche che cercano di manipolare il confronto pubblico senza rinunciare ai principi di libertà e pluralismo che intendono proteggere.

L'Europa ha iniziato a costruire gli strumenti per farlo. I prossimi appuntamenti elettorali diranno quanto siano diventati efficaci. E soprattutto se l'Italia avrà deciso di considerare finalmente la sicurezza del proprio spazio informativo una componente essenziale della sicurezza nazionale, anziché un problema da affrontare soltanto quando un'interferenza è già stata individuata.

??

internazionale/esteri

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione

Ottobre 20, 2026

Autore

redazione

default watermark