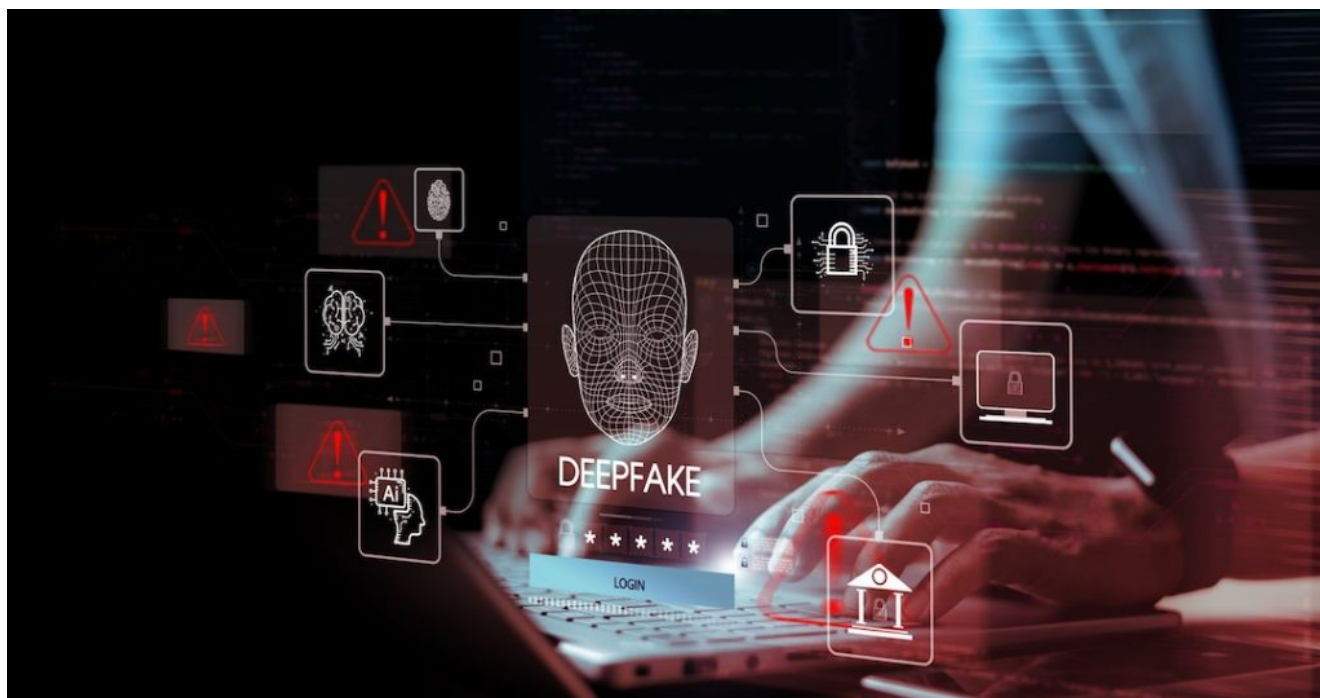


Deepfake al voto, l'Italia ha un'opportunità di leadership europea



Un candidato al Senato americano guarda dritto in camera, sorridente davanti alla bandiera del Texas, e pronuncia frasi che non ha mai detto. Il video è un falso generato dall'intelligenza artificiale, pubblicato dal comitato elettorale nazionale dei repubblicani. In basso a destra, in caratteri che nessuno legge, la scritta «AI generated». È successo poche settimane fa, nel pieno della campagna per le elezioni di metà mandato americane. Il candidato si chiama James Talarico, e le parole che gli sono state messe in bocca sono state costruite montando vecchi post sui social. Ma chi guarda il video non lo sa. Vede un uomo, sente una voce, e ci crede. Questo non è uno scenario da fantascienza, ma il presente. E soprattutto il futuro, se nessuno interviene. In Italia, quarantaquattro milioni di persone sono attive sui social e, secondo i dati di Agcom, una su due si informa online. Non siamo immuni: siamo esposti. A novembre 2025 un video deepfake ha mostrato la presidente della Regione Umbria,

Stefania Proietti, inseguita da una folla inferocita. Non era opera di un troll anonimo, ma di un esponente politico. Ci sono stati deepfake contro esponenti di tutti gli schieramenti: Donzelli, Tajani, Santanché da una parte, Salis dall'altra. Le immagini generate dall'intelligenza artificiale vengono già utilizzate nella propaganda di diversipartiti. Tutti hanno firmato un impegno volontario a non usare deepfake contro gli avversari. Ma un impegno volontario senza sanzioni è una stretta di mano senza contratto: vale finché conviene. Il problema non ha colore politico, e la soluzione nemmeno. L'Italia ha già fatto un primo passo importante: la legge 132 del 2025 sull'intelligenza artificiale ha introdotto il reato di deepfake, con pene da uno a cinque anni per chi diffonde contenuti manipolati senza consenso. È una base solida.

Ma un processo penale ha tempi incompatibili con quelli di una campagna elettorale. Se un deepfake del mio avversario circola nell'ultimo fine settimana prima del voto, il processo inizierà quando le urne saranno chiuse da mesi. La sentenza arriverà troppo tardi per rimediare il danno.

Per completare il quadro serve un meccanismo amministrativo rapido, con l'Agcom nel ruolo di arbitro e la possibilità di ordinare la rimozione di un contenuto falso entro ventiquattro ore. Non la satira, non la parodia dichiarata: solo i contenuti fabbricati per ingannare l'elettore. Una legge del genere non limita la libertà di espressione, la difende: perché un elettore ingannato non è un elettore libero.

Chi pensa che il problema sia teorico guardi agli Stati Uniti, dove nessuna legge federale regola l'uso dell'IA nella comunicazione politica. Il disastro è già in corso, come documenta un'inchiesta della Reuters di pochi giorni fa. Oltre al caso Talarico, la campagna di un candidato repubblicano della Georgia ha fabbricato un deepfake del senatore Jon Ossoff, facendogli pronunciare parole mai dette sull'agricoltura e sullo shutdown del governo. Solo ventotto stati su cinquanta hanno leggi in materia, e nella maggior

parte dei casi l'obbligo si riduce a una scritta in corpo minuscolo 2 nell'angolo di un video che scorre su uno smartphone. Uno studio del 2025 pubblicato sul Journal of Creative Communications ha confermato ciò che tutti sospettano: le persone non riescono a distinguere i deepfake dai video autentici, e ne sono influenzate. Le piattaforme, intanto, hanno smantellato i sistemi professionali di fact-checking. L'Europa si muove: il Parlamento europeo ha appena fissato a novembre 2026 la scadenza per il watermarking dei contenuti generati dall'IA, riducendo i tempi rispetto alla proroga più lunga proposta dalla Commissione. L'obbligo di etichettare audio, video e testi sintetici sarà vincolante. Ma il watermarking non basta: serve anche la possibilità di rimuovere rapidamente i contenuti prodotti per inquinare una campagna elettorale. Nessun paese europeo ha ancora una legge del genere. La normativa sulla propaganda elettorale risale al 1956, quando il peggior attacco alla democrazia informativa consisteva in un volantino ciclostilato. Il governo italiano ha l'occasione di colmare questo vuoto per primo, costruendo sulla legge 132 già approvata e completandola con uno strumento amministrativo rapido ed efficace. Il Parlamento ha già esplorato questa direzione con una proposta di legge che prevedeva proprio il ruolo dell'Agcom come garante: non è passata, ma il lavoro preparatorio c'è e può essere messo a frutto.

L'Italia va alle politiche nel 2027. Mancano meno di due anni. La tecnologia per creare un deepfake indistinguibile dal vero costa poche decine di euro, richiede pochi minuti e competenze elementari. Tra un anno, che in informatica equivale a un decennio, la situazione si sarà molto aggravata. Approvare una legge che vada in questa direzione (condivisa, trasversale, perfezionata insieme) significherebbe proteggere l'elettore, cioè tutti. Non è una questione di destra o di sinistra: un deepfake avvelena il dibattito indipendentemente da chi lo produce e da chi lo subisce. Un'Italia che approva per prima in Europa una legge contro i deepfake elettorali si presenta

ai tavoli internazionali con un argomento in più, in un momento in cui gli Stati Uniti mostrano al mondo quanto costa non avere regole. Sarebbe un risultato spendibile ovunque, e un ottimo segnale, in Europa e nei rapporti bilaterali. Ma soprattutto sarebbe il modo migliore per arrivare alle politiche del 2027 con la certezza che la competizione elettorale si giochi sulle idee, non sulle falsificazioni.