FRODI ONLINE Con i falsi creati con l'intelligenza artificiale in soli otto mesi sono stati rubati agli italiani 116 mln di euro. Faro della Polizia Postale sui deepfake: ci sono metodi di smascherarli ma servono nuove regole

Gli insoliti ignoti

di **Anna Di Rocco** e **Silvia Valente**

Nel video c'era la presidente del Consiglio: stessa voce, stessi gesti, persino le espressioni familiari. Presentava Quantum, un progetto di investimento garantito dallo stato che permette di guadagnare tra i 40 e i 50 mila euro in pochi mesi a fronte di un versamento di 250 euro. Solo che non era davvero lei. Si trattava di un deepfake: un falso video realizzato attraverso l'intelligenza artificiale. «Potremmo definirla una truffa online versione 5.0, gestita interamente con l'AI, e perpetrata sempre più frequentemente anche nel

Ivano Gabrielli
Polizia Postale

nostro Paese», spiega a *MF-Milano Finanza* il direttore della Polizia Postale, Ivano Gabrielli. E a dimostrarlo sono i numeri.

Nei primi otto mesi del 2025 sono stati trattati 12 mila casi di truffe informatiche, per un totale di 143 milioni di euro sottratti alle vittime. «Il falso trading online si conferma senza ombra di dubbio la truffa online più redditizia: sebbene i casi rappresentino il 29% del totale assorbono l'81% delle somme sottratte, pari a oltre quattro quinti delle perdite economiche del periodo. Attraverso questa pratica, solo tra gennaio e agosto, i truffatori sono riusciti a sottrarre 116 milioni di euro ai malcapitati, cifra in crescita del 15% rispetto allo stesso periodo dell'anno precedente. «A favorirne la proliferazione», spiega il direttore Gabrielli, «è la bassa alfabetizzazione finanziaria, combinata con campagne ingannevoli talvolta potenziate dal deepfake».

«Al contrario di quel che si potrebbe pensare chi incappa in queste tipologie di truffe ha un'istruzione medio-alta e, ovviamente, disponibilità economiche importanti», spiega ancora il responsabile della Polizia Postale. «Molto spesso il percorso di investimento è oggettivamente credibile. Una prima fase di piccoli versamenti vincenti crea fiducia e incoraggia investimenti via via più consistenti: è in questo momento che la truffa si perfeziona: la piattaforma smette di funzionare, il broker diventa irreperibile e il capitale viene perso. La modalità d'esecuzione si combina poi con la psicologia. Si tratta di un percorso traumatico per la vittima e i truffatori sfruttano più e più volte sulla vulnerabilità delle persone». E questo si riflette nelle denunce che «avvengono o all'inizio della frode o alla fine, grazie all'aiuto di un familiare o di un affetto. Di contro questo genera un enorme difficoltà nel recupero delle somme da parte della Polizia».

Spaventa, in tutto questo, l'utilizzo smodato dell'intelligenza artificiale per perpetrare la truffa. «Dietro ci sono attività riconducibili a organizzazioni criminali, spesso di stampo internazionale», segnala Gabrielli, ricordando i recenti interventi per bloccare distretti frodatori in Italia, Albania e nel Sud est asiatico. «Il problema è che il deepfake può rendere la truffa estremamente sofisticata: sfruttando l'AI sono stati riprodotti illegalmente siti di testate giornalistiche online necessari per diffondere video promozionali di investimenti finanziari o di trading online. In altri casi i deepfake vengono diffusi sui social network per raggiungere un numero maggiore di potenziali vittime».

Nel corso dell'anno anche il ministro dell'Economia, Giancarlo Giorgetti, ne è stato vittima con un video che sfruttava la sua immagine per pubblicizzare piattaforma abusive di trading. E non è l'unico, tempo fa finì clonato anche il governatore della Banca d'Italia Fabrio Panetta. I cybercriminali hanno usato l'immagine della premier Giorgia Meloni e il volto del presidente della Repubblica, Sergio Mattarella, nonché quello di Giovanni Ferrero, il patron dello storico marchio italiano. Senza dimenticare che la Consob ha recentemente bloccato il sito Finivestonline.com che diffondeva pubblicità sul web per offrire servizi finanziari abusivi, facendo leva sui marchi Fininvest-Mediaset e su alcuni membri della famiglia Berlusconi.

L'azione delle Autorità è fondamentale: la Polizia Postale e Agcom possono essere attivati al primo contatto, la Consob ha il potere di oscurare i siti fraudolenti, l'Antitrust interviene contro pratiche commerciali scorrette e poco trasparenti, il Garante della Privacy agisce a difesa della tutela dei dati personali. Molto però resta nella capacità dei cittadini di non cadere nelle truffe architettate dai criminali digitali. Riconoscere i deepfake può essere sfidante ma ci sono alcuni piccoli segnali che possono aiutare le persone ad accorgersene prima di diventare vittime, come suggerisce la Polizia postale sul suo sito. Se i movimenti degli occhi, battito delle ciglia, la direzione dello sguardo, sono innaturali o se in generale il corpo e la postura sono rigidi, si deve accendere un campanello d'allarme.

Bisogna inoltre prestare attenzione ai movimenti della bocca e alla sincronizzazione tra voce e labbra, difficile da rendere perfetta con l'AI. Sempre restando con la lente d'ingrandimento sulla zona della bocca, notare la definizione dei

COME RICONOSCERE UN DEEPFAKE

Foto generata con ChatGpt in versione gratuita

Foto reale

COME RICONOSCERE IL VERO DAL FALSO?

1. Controllare i movimenti degli occhi
2. Controllare i denti e la sincronizzazione voce-movimento labbra
3. Controllare la postura
4. Controllare le luci e le ombre
5. Verificare la presenza dei tratti distintivi della persona, come colore dei capelli, baffi, barba e abbigliamento

Perché l'Europa deve evitare la retorica della «sovranità digitale»

di **Oreste Pollicino***

Non è la prima volta che Stati Uniti ed Europa si affrontano sul digitale. Eppure questa volta l'impressione è che lo scontro vada oltre il solito scambio di accuse. Donald Trump, fedele al suo stile diretto, ha bollato le norme europee come un attacco alle «incredibili aziende americane» e ha minacciato tariffe pesanti. Da Bruxelles la risposta è stata immediata: l'Unione decide in piena autonomia come regolare il proprio mercato interno. Una frase semplice, che in realtà suona come una dichiarazione di sovranità.

Dietro questo botta e risposta c'è una verità meno comoda. Le regole europee - il Digital Markets Act (Dma) e il Digital Services Act (Dsa) - nascono con l'intento di essere generali e neutrali. Limitare gli abusi di potere delle piattaforme, imporre trasparenza sui contenuti, ridurre disinformazione. Ma dall'altra parte dell'Atlantico la percezione è diversa: leggi costruite per frenare i colossi americani, mascherate da tutela dei consumatori. È qui che si vede un limite strutturale dell'Unione: proclamare neutralità è più facile che convincere partner globali e mercati del fatto che quella neutralità esista davvero.

Il problema è che l'Europa spesso non aiuta se stessa. Le decisioni arrivano con tempi lunghissimi, i meccanismi di attuazione sono farraginosi, le autorità nazionali si muovono in ordine sparso. Basta guardare alle prime applicazioni del Dma: grandi annunci, poche decisioni realmente incisive. Così il rischio è duplice: gli Stati Uniti vedono barriere nascoste, mentre i cittadini europei percepiscono una macchina normativa lenta e distante.

Il gdpr resta l'eccezione. Criticato all'inizio come ostacolo per le imprese, è diventato un benchmark globale. Ma non tutte le partite sono uguali. Il pacchetto digitale - Dsa, Dma e ora l'AI Act - richiede una capacità di enforcement che oggi Bruxelles non ha pienamente dimostrato. Servono risorse, chiarezza e tempi rapidi. Senza questi elementi, la retorica della «sovranità digitale» rischia di restare un titolo di conferenza più che una realtà politica.

Ursula von der Leyen

La minaccia di tariffe americane arriva proprio mentre l'AI Act si prepara a entrare in vigore. Qui l'Europa ha una finestra di opportunità: costruire un modello che altri possano seguire. Ma questa opportunità può svanire se l'Unione continua a oscillare tra ambizione e indecisione. È difficile convincere che sull'AI le regole non siano merce di scambio se, allo stesso tempo, si mostra debolezza nel difendere Dsa e Dma.

La vera domanda allora non è se l'Europa abbia il diritto di legiferare - quello è fuori discussione - ma se abbia la capacità di farlo in modo credibile, rapido e coerente. Perché la credibilità non si misura nelle dichiarazioni ufficiali, ma nella capacità di resistere alle pressioni, applicare le norme senza distinzioni di bandiera, correggere gli errori senza impantanarsi in procedure infinite.

L'Europa deve scegliere: vuole essere solo un grande mercato da difendere, o un soggetto capace di scrivere regole che valgono anche fuori dai suoi confini? Nel primo caso resterà subalterna, nel secondo potrà trasformare il digitale in banco di prova della propria sovranità. Ma per farlo deve prima guardarsi dentro, ridurre la distanza tra Bruxelles e operatori economici, tra principi proclamati e decisioni reali.

Il digitale non aspetta. E se l'Unione continuerà a parlare più che agire, saranno altri - Washington o Pechino - a dettare la rotta. In quel caso, non basterà ricordare il successo del gdpr. Servirà spiegare ai cittadini perché la "sovranità digitale" si è fermata alle parole.

**Ordinario di diritto della regolamentazione dell'AI, Università Bocconi. Founder Pollicino Aidvisory*