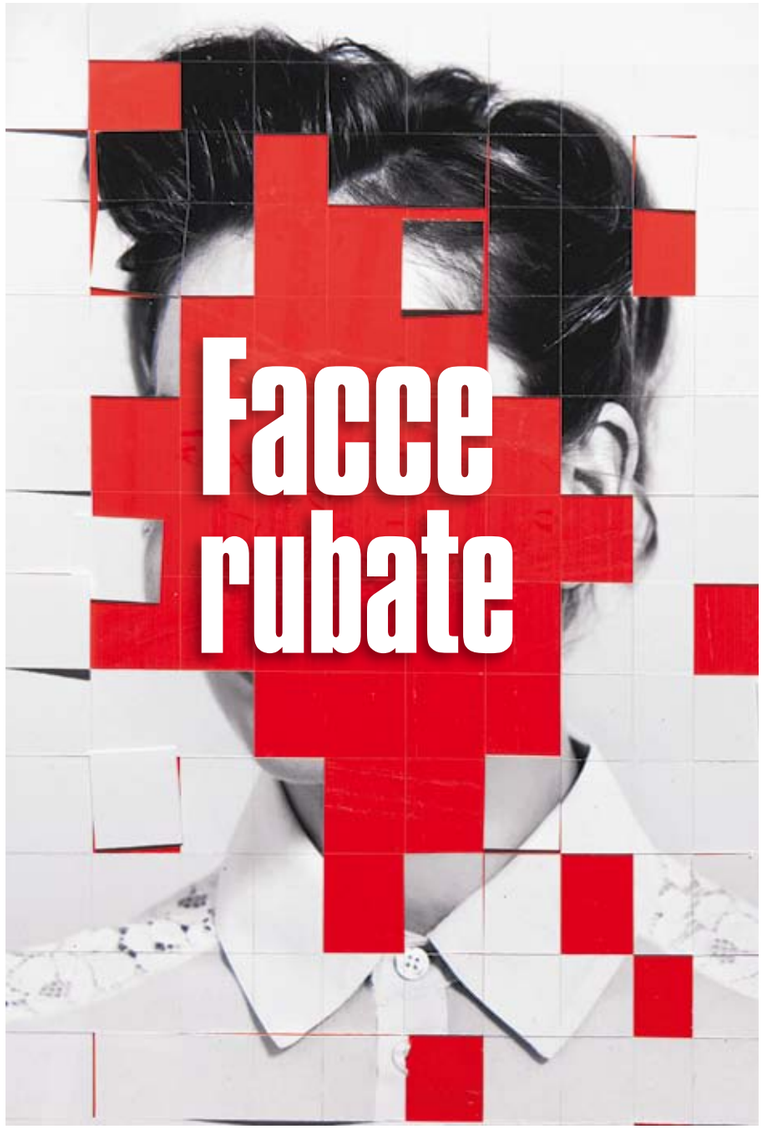
**La nuova frontiera nel furto d'identità digitale è quella del «deepfake», con la manipolazione del volto e della voce di una persona, possibilmente famosa. Foto e video contraffatti diventano così strumento di ricatto e mistificazione politica.**




Getty Images

*di Stefano Piazza*
*e Luciano Tirinnanzi*

**GIORGIA MELONI** protagonista di un film porno. Barack Obama che dà dello «stronzo» a Donald Trump. Tom Cruise che fa lo scemo sul TikTok. No, non sono allucinazioni visive o invenzioni da giornalisti. Si chiama «deepfake», ed è la nuova preoccupante evoluzione delle fake news, le notizie fasulle. O meglio, la loro «involuzione» tecnologica. In pratica, l'ultima frontiera del furto d'identità digitale: una tecnica sofisticata che si basa sulla manipolazione del volto e della voce di una persona, per creare online nuovi contenuti verosimili, ma del tutto falsi.

Una moda social che punta a mettere in bocca a personaggi influenti frasi che non corrispondono minimamente al loro pensiero, ingannando così la buona fede del pubblico e alimentando la disinformazione allo scopo di screditarli e influenzare le opinioni. I risultati di questi «scherzi» possono essere devastanti e dalle conseguenze imprevedibili: l'assalto al Campidoglio dei fan di Trump insegna che una sola parola, se distorta, può generare caos e violenza.

Ivan Bracco, dirigente del sindacato di Polizia Sap con una lunga esperienza investigativa nella Polizia postale e delle comunicazioni, spiega: «Inizialmente, foto e video contraffatti erano quasi esclusivamente relativi al revenge porn, cioè a quel fenomeno dove per vendetta o per ricatto si utilizzano immagini e video pornografici alterati dove, al posto dell'attrice di turno, figura magari la propria ex. Oggi siamo ben oltre. Perché non si tratta più di semplici fotomontaggi o di "copia e incoll" più o meno accurati, ma di veri contenuti inediti frutto dell'intelligenza artificiale».

Il problema è che questa tecnologia non è così complessa da richiedere le competenze di un informatico o un hacker. «Al contrario, reperire software gratuiti per creare deepfake è facile e alla portata di tutti. Inoltre, le app in circolazione che permettono questa sofisticazione sono così accurate da garantire risultati sbalorditivi anche a un livello base».

Ricordate le app che permettono di invecchiare un volto grazie a un semplice filtro che ritocca le foto? Quello era l'anno zero del deepfake. Ormai gli algoritmi che generano clip e video artefatti attraverso l'uso dell'intelligenza artificiale sono così evoluti da essere in grado non soltanto di modificare agilmente immagini e audio originali, ma anche di simulare, riprodurcendoli, i caratteri e persino i movimenti del corpo di un soggetto, fino a imitarne quasi perfettamente la sua voce. E può riuscirci anche un bambino.

**«Siamo molto preoccupati per le prossime campagne elettorali»** aggiunge l'esperto. «Perché è sempre più arduo gestire i numerosi flussi di comunicazione che i vari partecipanti caricano sui social, dove già di per sé è difficile risalire al primo anello della catena per contestare un'ipotesi di reato. Inoltre, la maggior parte dei social, così come i gestori dei server e dei dati, sono stranieri. Per la nostra Polizia postale risalire agli autori di tali crimini informatici è perciò estremamente difficile».

Lo scorso 10 marzo 2021, non a caso, la divisione informatica americana dell'Fbi ha allertato sulla minaccia concreta portata da attori stranieri che «quasi certamente faranno leva sui contenuti sintetici per le operazioni di influenza cibernetica nei prossimi 12-18 mesi». Allarme scattato dopo il caso della (finta) speaker della Camera, Nancy Pelosi, ripresa ubriaca in un video amatoriale, cui hanno fatto seguito altri episodi legati a personaggi politici minori.

Dopo che anche in Italia abbiamo avuto il primo caso di un politico vittima di deepfake - i «ladri del volto» di Giorgia Meloni sarebbero due sassaresi, accusati del reato di diffamazione per aver pubblicato il citato porno con protagonista «l'avatar» della leader di Fratelli d'Italia - anche il nostro governo ha preso le contromisure. Palazzo Chigi ha, infatti, istituito un organo di sorveglianza denominato Csirt, Computer security incident response team: «Una squadra che si occupa di cyberdifesa e di valutare nel flusso di informazioni, incidenti di tipo informatico, di sicurezza generale delle informazioni e di natura fisica legati alla gestione degli asset» spiega Marco Santarelli, esperto in analisi delle reti, infrastrutture critiche, intelligence e big data.

La manipolazioni «deepfake» dell'immagine di Tom Cruise sul social TikTok è opera di un artista, il belga Chris Ume.

Ma non basta. Serve una legislazione ad hoc, che però ancora manca. Anche perché le implicazioni del deepfake sono talmente estese e gravi da sconfinare quasi sempre nell'illegalità: la perdita di controllo della propria immagine, così come la deformazione delle proprie idee e opinioni, possono infatti avere conseguenze inimmaginabili sui vari soggetti che la subiscono: distruggere del tutto la reputazione di una persona compromettendo le sue relazioni sociali, il lavoro e la carriera, può spingerla fino al suicidio.

Ne è convinto lo stesso il Garante della privacy, secondo cui il rischio connesso all'utilizzo di questa tecnologia è proprio quello di «rappresentare una grave minaccia per la riservatezza e la dignità delle persone». Perché il deepfake può «privare le persone della cosiddetta autodeterminazione informativa (ciò che voglio far sapere di me lo decido io), come pure incidere sulla loro libertà decisionale (quello che penso e faccio è una scelta su cui gli altri non possono interferire)».

**Non solo, grazie all'intelligenza artificiale già oggi si potrebbe far dichiarare** al presidente degli Stati Uniti di voler bombardare un Paese straniero. O mettere in bocca a Papa Francesco parole di odio verso le minoranze etniche. Ma il deepfake coinvolge anche le persone comuni, che sempre più spesso si scoprono vittime di: deepnude (persone ignare rappresentate svestite a letto con l'amante o in contesti degradanti); del citato revenge porn (a scopo ricattatorio-denigratorio); di cybercrime (per ingannare i sistemi di sicurezza basati su riconoscimenti vocali e facciali); fino al cyberbullismo e alla pedopornografia.

Certamente, i più avveduti riconosceranno l'artificiosità di tali clip. Ma fino a che punto? E fino a quando? Ormai, gli stessi giornalisti non sembrano più in grado di distinguere sempre e comunque il falso dal vero: come dimostrano i clamorosi falsi scoop di Claas Relotius per lo *Spiegel*, che lo stesso magazine tedesco ha definito «il punto più basso della nostra storia lunga oltre settant'anni»; o come la testimonianza di un falso militante dell'Isis premiata e osannata dal *New York Times*, ma poi rivelatasi opera di un impostore. Come per le più note fake news, la conseguenza per tutti è che, una volta online, specie se virale il falso digitale non si può cancellare, né una rettifica sarebbe sufficiente a contenere i danni. ■