Dossier e ricatti: la fabbrica dei deepfake cresce del 550%

Cripto crimine. Nel 2023 i video falsificati con l'Ia finiti online sono stati 95.820. Allarme Consob: influenzate le scelte degli operatori economici

Pagina a cura di
Margherita Ceci
Ivan Cimmarusti

Nel 2023 i video *deepfake* presenti sul web sono stati 95.820, in aumento del 550% rispetto al 2019. Ma un tracciamento reale non è cosa facile. Ogni giorno i social sono inondati di questo tipo di messaggi generati con l'Intelligenza artificiale (Ia). L'ultimo finito in circolazione riguarda la premier Giorgia Meloni – affiancata da Elon Musk e dal direttore del Tg La7 Enrico Mentana — che promuove una piattaforma di *trading online* per guadagni fino a 40mila euro al mese. In alcuni casi sono poco credibili, ma possono ugualmente influenzare le scelte finanziarie, a maggior ragione se creati ad hoc per colpire un obiettivo prestabilito. Come quel dirigente di Arup, società inglese di design e ingegneria, che ha pagato 25 milioni di dollari a un cybercriminale dopo una falsa videochiamata aziendale generata con l'Ia.

> **I filmati falsi dell'ad di Eni Descalzi e del governatore di Bankitalia Panetta su investimenti finanziari opachi**

Un aspetto difficile da intercettare che sta allarmando gli apparati di sicurezza. I rischi non sono solo le distorsioni del mercato. C'è anche la creazione di dossier (si veda l'articolo a destra) basati su informazioni falsificate, ma credibili, e la manipolazione delle prove processuali.

Di quest'ultimo aspetto parla Martino Jerian, di Amped Software. «Ad oggi, una volta che un'immagine viene analizzata in maniera accurata da un esperto, è abbastanza difficile che venga scambiata come reale e usata come materiale probatorio. Il rischio che c'è in realtà è più sottile, ed è il fatto di utilizzare l'Ia per migliorare le fonti di prova. Oggi è possibile avere l'immagine di una faccia da tre pixel e tirarne fuori un volto perfetto: ma quando io miglioro un'immagine con Ia, di base ho un *deepfake*». E aggiunge: «Abbiamo fatto diverse prove qualche anno fa con dei volti di celebrità. Abbiamo visto che il risultato dava una forma degli occhi diversa da quella reale, toglieva i nei, cambiava la forma delle orecchie (che è un dettaglio molto distintivo nelle persone). E si sta iniziando a prendere coscienza del problema: quest'anno c'è stato per la prima volta un grosso caso negli Stati Uniti in cui un video migliorato con l'Ia è stato dichiarato non utilizzabile dal giudice per questo motivo».

Il tema, si diceva, è sotto l'attenta analisi dei Servizi di sicurezza italiani, soprattutto per i risvolti che il deepfake può avere sulla nostra economia. Si pensi che a luglio scorso la Banca d'Italia ha informato che sul web continuano a essere pubblicati video falsi generati con l'Ia in cui è riprodotta la voce del Governatore Fabio Panetta. Messaggi che possono incrinare l'andamento di un sistema finanziario, influendo sulla Borsa. Non solo: nel corso di quest'anno la Polizia postale ha già oscurato oltre 470 siti web che promuovevano investimenti generati con *deepfake*, come quello dell'ad di Eni, Claudio Descalzi. «Questo tipo di truffa – ha spiegato la Polizia postale, diretta da Ivano Gabrielli – produce ogni anno un guadagno illecito di milioni di euro». Secondo le stime di Deloitte, solo negli Stati Uniti le perdite finanziarie causate da *deepfake* passeranno da 12,3 miliardi di dollari nel 2023 a 40 miliardi entro il 2027. Un tasso di crescita annuo del 32%.

Per la Consob, in caso di *deepfake* generati con Ia diventa «importante, come per le altre *fake news*, la velocità con cui i soggetti coinvolti, cioè in primo luogo le persone lese, ma anche i giornalisti e i media, riescono a rivelare al pubblico l'errore così da limitare la durata dell'impatto sui prezzi di mercato». L'Autorità di vigilanza dei mercati finanziari aggiunge che «la semplice idoneità delle dichiarazioni non veritiere a produrre effetti sui mercati rende le stesse illecite e sanzionabili, indipendentemente dall'eventuale finalità ludica del *deepfake* e, più in generale, dalla circostanza che gli autori del *deepfake* intendano o meno manipolare il prezzo di uno o più strumenti finanziari».

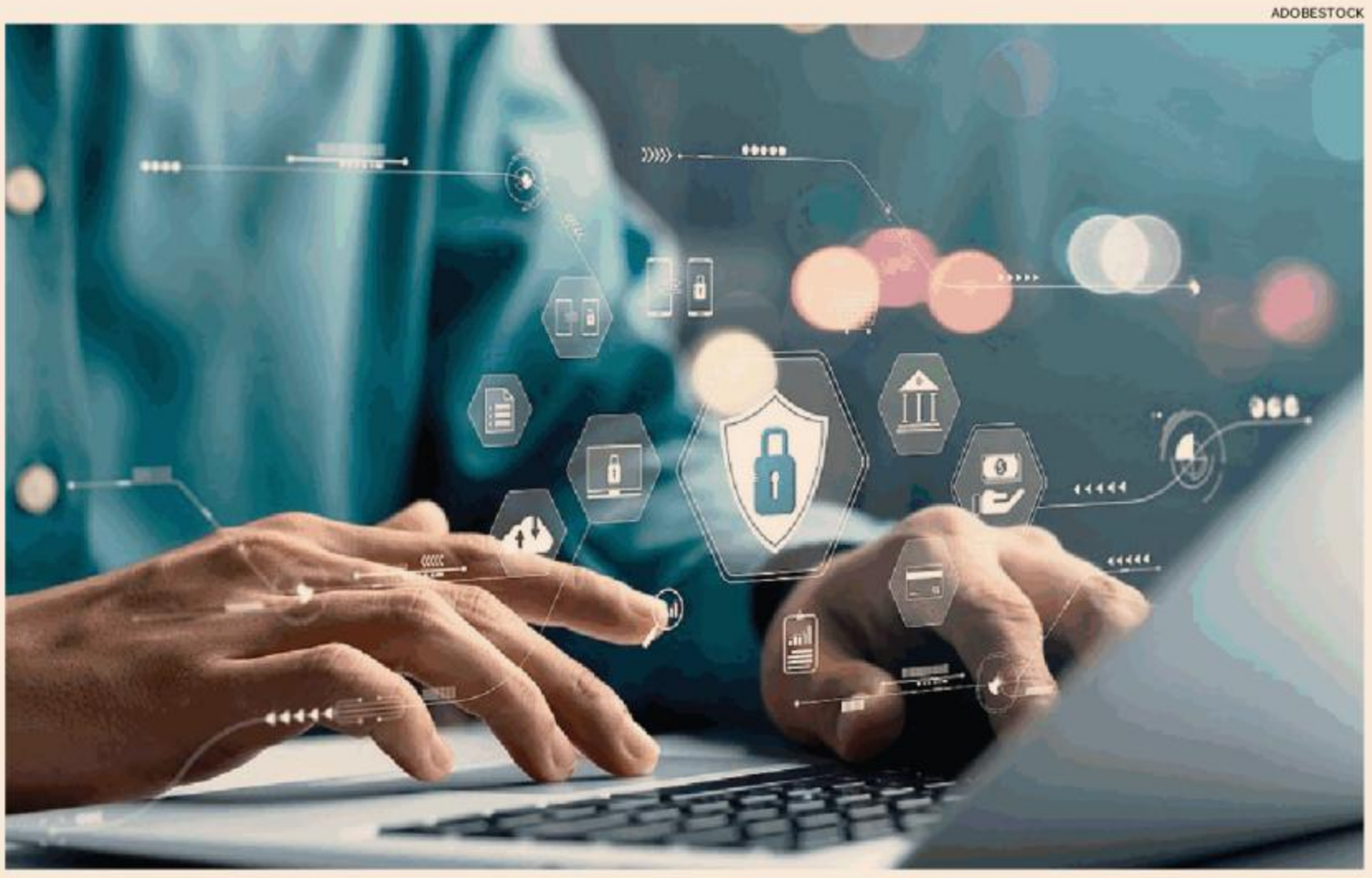
A giovarsi dell'accessibilità del *deepfake* è soprattutto l'industria della pornografia. Di quei 95.820 contenuti online registrati nel 2023, il 98% era di tipo pornografico. I dati arrivano dallo studio dell'Istituto internazionale delle Nazioni unite per la ricerca sul crimine e la giustizia (Unicri) in collaborazione con Bracket Foundation e Value for Good. Non solo: il National Center for Missing & Exploited Children (Ncmec), che raccoglie le segnalazioni di abusi su minori, riporta 36 milioni di avvisi ricevuti nel 2023. Di questi, 4.700 facevano riferimento a video generati con l'Ia.

Volti di persone o bambini presenti sul web fanno parte dei *data set* usati per allenare le intelligenze artificiali, finendo così per essere i protagonisti inconsapevoli di materiale pornografico. Il rischio di questa facilità nella creazione di contenuti è quello della normalizzazione.

I RIFLESSI LEGALI

Illeciti anche se per gioco
Il deepfake, anche creato con finalità ludiche, è considerato un illecito, e dunque sanzionabile, se le dichiarazioni false in esso contenute possono avere effetti sui mercati. A chiarire quest'aspetto è la stessa Autorità di vigilanza dei mercati finanziaria, che precisa come il fatto sia da dichiararsi reato a prescindere che «gli autori del deepfake intendano o meno manipolare il prezzo di uno o più strumenti finanziari».

ADOBESTOCK



Rischio forense. La giustizia inizia a porsi il problema dell'attinenza alla realtà delle immagini probatorie ricostruite tramite la

Il fenomeno

Abusi su minori
L'ultimo monitoraggio dell'Internet Watch Foundation su un forum del *dark web* ha registrato a luglio oltre 3.500 nuove immagini di abusi sessuali su minori generate dall'Ia rispetto alla precedente rilevazione del ottobre 2023. L'aumento è attribuito a una maggiore facilità di accesso, a modalità sempre più sicure e a basso costo di archiviazione digitale e alla maggiore accessibilità delle reti *peer-to-peer* e *deep web*.

470 siti web oscurati
Il fronte investigativo sul *deepfake* è caldo. Secondo gli ultimi dati disponibili del 2024 della Polizia postale, organismo diretto da Ivano Gabrielli, a oggi sono stati oscurati oltre 470 siti web che promuovevano investimenti finanziari falsi. In particolare, video generati con l'Intelligenza artificiale che riproducevano messaggi di importanti manager di Stato venivano utilizzati per indirizzare capitali.

Centrale del dossieraggio
L'inchiesta della Procura di Milano sulle società che si sarebbero occupate di creare dossier illeciti, ha dimostrato che hacker entravano nei telefoni cellulari dei target, cioè le vittime dell'attacco, per esfiltrare dati e informazioni sensibili che in alcuni casi venivano manipolati allo scopo di diffondere informazioni false. Con il materiale raccolto venivano quindi creati dei veri e propri dossier per colpire imprese e persone.