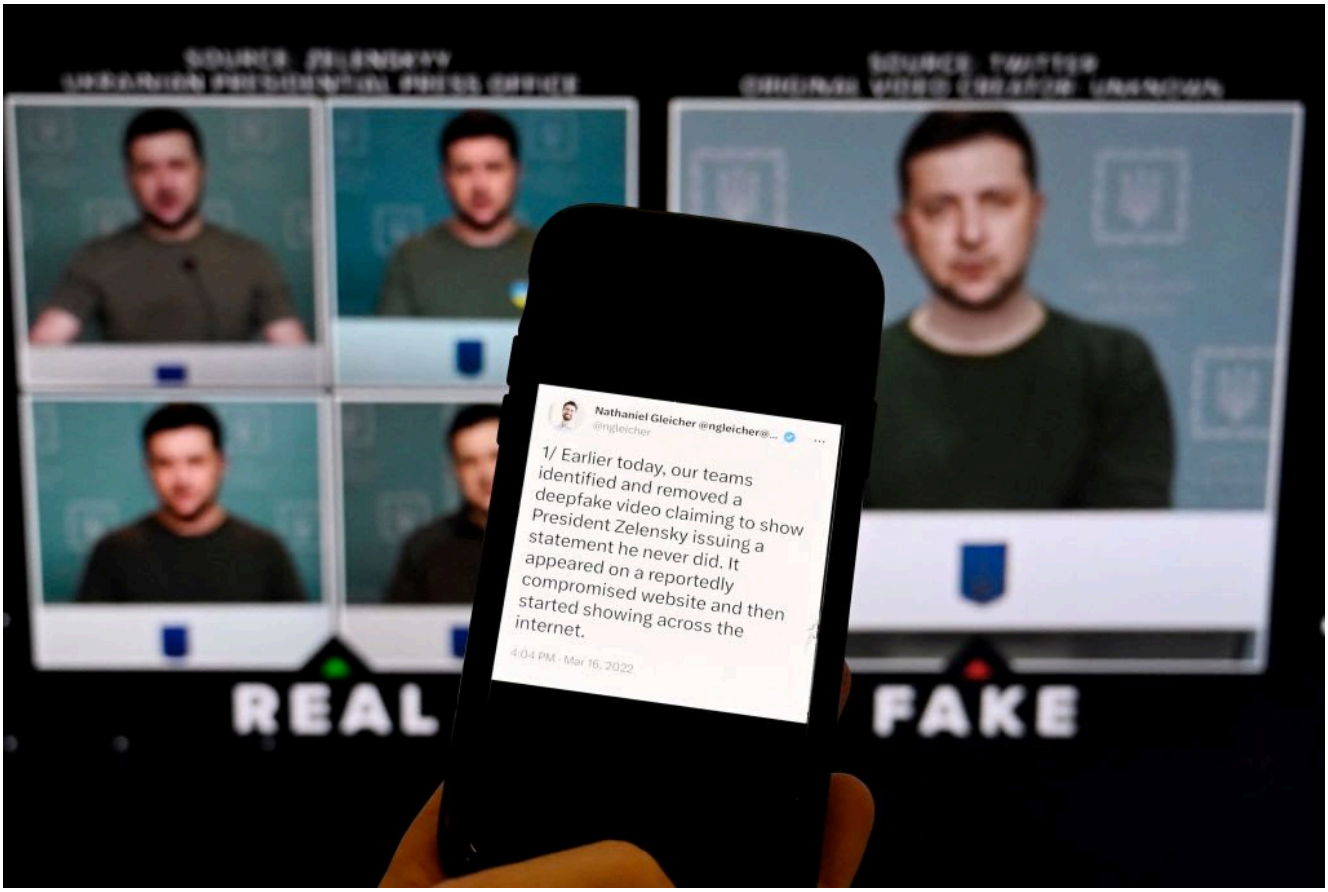
Deepfake: cosa sono, chi ne è stato vittima e come riconoscerli



Negli ultimi giorni in molti possono essersi imbattuti in un annuncio pubblicitario sui social che mostra una donna identica ad **Emma Watson** in atteggiamenti provocanti che richiamano quelli di un filmato porno. Ma la protagonista non è la celebre attrice britannica: il video è infatti parte di una campagna promozionale di un'applicazione **deepfake** che consente di sostituire il protagonista di un filmato con qualunque altro reperibile in rete, come nel caso di Watson. Molto usato per realizzare contenuti pornografici, questa campagna dimostra chiaramente come il deepfake si stia diffondendo anche su applicazioni di consumo alla mercé di tutti.

i got this ad yesterday and wow what the hell

> *pic.twitter.com/smGiR3MfMb*
>
> *— Lauren Barton (@laurenbarton03) March 6, 2023*

Cos’è e come viene usato il deepfake

Il deepfake è una tecnica che permette di creare video falsi ma abbastanza realistici da trarre in inganno. Si fa infatti ricorso all’apprendimento automatico che sfrutta l’intelligenza artificiale per **ricreare in maniera artificiosa il volto e la voce di una persona**, sovrapponendoli poi a un video esistente. La principale applicazione di questa tecnica è quella dei video a sfondo sessuale: un rapporto del 2019 di **DeepTrace**, una società con sede ad Amsterdam che monitora i media online, ha infatti rilevato che il **96%** del materiale deepfake in rete è di **natura pornografica.** Ma il deepfake può anche essere utilizzato per diffondere notizie false o compiere atti di cyberbullismo e vari altri crimini informatici.

Se fino a poco tempo fa per realizzare questo tipo di contenuti erano necessari **programmi sofisticati e a pagamento**, adesso l’operazione sta diventando sempre più semplice anche per gli utenti comuni, dal momento che i *reel* di Instagram o i video di TikTok offrono agli utenti i volti di milioni di individui, famosi e non, da poter ‘sfruttare’ e le app che consentono la manipolazione del materiale anche senza approfondite conoscenze informatiche.

Casi celebri: da Zelenski a Matteo Renzi e Barack Obama

Diversi personaggi pubblici si sono purtroppo ritrovati in situazioni spiacevoli a causa dei deepfake, come nel caso di politici apparsi in video nei quali sembravano pronunciare parole che in realtà non avevano mai detto. Pochi giorni dopo

l'inizio dell'invasione russa, lo stesso presidente ucraino **Volodymyr Zelensky** ne fu vittima. Un video mal riuscito lo ritraeva mentre si rivolgeva ai suoi soldati, incoraggiandoli ad arrendersi. Nonostante il falso fu subito smascherato, (il labiale era ben sincronizzato, ma l'accento di Zelensky era sbagliato, la sua testa troppo grande e con una risoluzione diversa rispetto al corpo e allo sfondo), quelle immagini fecero suonare un campanello d'allarme, per le potenziali dannose conseguenze della diffusione di questo tipo di contenuti se utilizzati per influenzare l'opinione pubblica. Anche i politici italiani non sono rimasti immuni al fenomeno: celebre era il caso di **Striscia La Notizia** che nel 2019 aveva realizzato un finto fuori onda di **Matteo Renzi** e **Matteo Salvini.**

Di deepfake si parla molto anche nel cinema, dove da tempo si discute se sia giusto utilizzarlo per 'ringiovanire' alcuni attori o addirittura 'riportarne in vita' altri, come accadde con il film di Star Wars *Rogue One* del 2016, quando il defunto **Peter Cushing** (1913-1994) è 'tornato' a interpretare il Grand Moff Tarkin grazie all'animazione digitale. Il regista premio Oscar **Jordan Peele**, per sensibilizzare sul tema, realizzò nel 2018 un deepfake dell'ex presidente **Barack Obama**, già allora molto credibile, a dimostrazione della crescente difficoltà di distinguere ciò che è vero da ciò che non lo è.

Limitazioni: in Cina posti dei paletti alla creazioni di video

Le preoccupazioni sui deepfake hanno portato ad una proliferazione di contromisure. Il 10 gennaio è entrata in vigore in Cina una nuova normativa volta a **disciplinare la creazione e la diffusione di contenuti ottenuti tramite le intelligenze artificiali generative**, compresi i deepfake. Alcune piattaforme social, tra cui Facebook e Twitter, li

hanno banditi dalle loro reti. E il **Garante della Privacy** nel 2020 mise a punto una scheda informativa per sensibilizzare gli utenti sui **rischi** connessi agli usi malevoli di questa nuova tecnologia.

Come riconoscere un deepfake

Seppure la qualità stia migliorando di giorno in giorno, smascherare un deepfake è ancora possibile: l'attuale tecnologia ha problemi ad animare realisticamente i volti ed il risultato è un video in cui il soggetto **non sbatte mai le palpebre** o lo fa troppo spesso e in modo innaturale. Si possono inoltre trovare anomalie per ciò che riguarda **la pelle ed i capelli**, oppure **volti che sembrano essere più sfocati** rispetto all'ambiente in cui sono posizionati. Anche la **luce** del video può rappresentare un indizio: spesso gli algoritmi di deepfake conservano l'illuminazione delle clip originali, che finiscono per non corrispondere a quella dei video a cui vengono sovrapposte. Infine sono spesso rintracciabili problemi relativi all'**audio,** che alle volte non emula adeguatamente la voce del protagonista o non viene manipolato con la stessa attenzione del video.