GRAZIA

diffusione:90239
tiratura:138244

[10 NOTIZIE]

QUELLA NELLO SCHERMO NON SONO IO

In Rete circolano sempre più video e foto che sembrano avere come protagonisti volti noti. Invece sono elaborazioni digitali non autorizzate, chiamate **"deepfake"**. Tra le ultime vittime c'è la pop star Rose Villain. *Grazia* ha indagato questo fenomeno che rende più difficile distinguere tra realtà e finzione

di Alessia Ercolini

1

LA CANTAUTRICE ROSE VILLAIN, 34 ANNI.

Foto MARCELLO DINO JUNIOR

L'ultimo caso è stato quello della cantante Rose Villain che pochi giorni fa è stata vittima di "deepnude", foto false diffuse in Rete in cui è nuda. **Per quelle immagini create con l'Intelligenza Artificiale Villain ha presentato una denuncia alla Polizia postale. A fine gennaio la più grande pop star americana, Taylor Swift, si è trovata in una situazione simile.** Immagini pornografiche della cantante sono diventate virali sui social, una di queste è stata vista 47 milioni di volte su X, prima che il profilo venisse sospeso. Si chiamano "deepfake", dall'unione di due termini inglesi, quello riferito alla tecnologia del "deep learning" (apprendimento profondo) con la parola "fake", cioè falso. In altre parole, l'Intelligenza Artificiale oggi viene usata per studiare il modo di muoversi e parlare delle persone e riesce a "impararli" e a riprodurli. Non si tratta di fotomontaggi, ma di contenuti video e audio verosimili che traggono in inganno.

Come possiamo riconoscere il falso dal vero? «Questo è solo l'inizio e con le classiche accortezze dal punto di vista tecnico è complicatissimo, perché **essendo l'Intelligenza Artificiale "generativa" (crea un'immagine nuova, *ndr*) non c'è una foto di partenza che dia un indice di falsità»,**

GRAZIA

diffusione:90239
tiratura:138244

spiega Giovanni Ziccardi, docente di Informatica giuridica all'Università degli Studi di Milano e autore di *Dati avvelenati. Truffe, virus informatici e falso online* (Raffaello Cortina). «La cosa che stupisce è la precisione di queste immagini: chi le ha viste non ha pensato a un falso perché erano indistinguibili dal vero. Non si tratta più della falsificazione con un programma che incolla la testa al corpo di un altro, bensì la creazione di contenuti completamente falsi. E ormai questa tecnologia è alla portata di tutti a un costo minimo. Dal ragazzino allo stalker o a chi vuole alterare gli equilibri democratici creando il falso, chiunque è in grado di farlo. Nel nostro centro di ricerca all'Università degli Studi di Milano ci occupiamo soprattutto dei crimini che vengono commessi con questi falsi: si va dallo stalking al cyberbullismo, ma ci sono anche tante frodi. **Tra gli ultimi casi c'è stata la finta riunione dei dirigenti di una multinazionale dove un impiegato era convinto di essere in un meeting con i suoi capi e ha fatto bonifici per 25 milioni di dollari.** Invece era con truffatori che con la tecnologia "deepfake" avevano assunto le sembianze dei dirigenti della società».

Come possiamo cautelarci di fronte a una tecnologia così potente? «La soluzione è aumentare l'alfabetizzazione digitale delle persone», dice Ziccardi. «Abbiamo l'idea che la nostra sia una società avanzata dal punto di vista tecnologico, invece risulta che una persona su due non abbia le competenze di base. Spesso le persone non hanno la minima competenza riguardo alla tecnologia che stanno utilizzando e questo le rende prede facili. Il primo rimedio è formare il cittadino per aumentarne la consapevolezza».

Dalle foto sui social agli scambi su WhatsApp, ogni giorno sui social circolano migliaia di nostre foto. Così è più facile che ci rubino l'identità? «Più di quanto si creda, **i "deepfake" possono colpire tutti», dice l'avvocata Alberta Antonucci, esperta di reati informatici e fondatrice di On The Web Side. «Io ho trattato un caso di "deepfake" a danno di un professore che si qualificava in un video come un pedofilo e innamorato di alcune sue studentesse.** Un altro caso recente ha riguardato l'app Bikinioff che permetteva di caricare delle semplicissime foto di persone scaricate da Instagram e spogliarle con risultati di "deepfake" molto realistici, tanto che, un anno fa, due quattordicenni sono stati accusati di aver prodotto materiale pedopornografico a danno delle proprie compagne di classe proprio con quella app».

Ci troviamo dunque di fronte a un nuovo tipo di reato? «C'è un vuoto normativo, al momento non esiste il reato di "deepfake", dobbiamo analizzare caso per caso, ovverosia come, quando e perché vengono utilizzati i "deepfake". Possono essere generati per fini di truffa, diffamazione e revenge porn. Già nel 2020 il Garante per la protezione dei dati personali ha avviato un'istruttoria nei confronti del social Telegram per un software che spogliava le donne, "Deepnude", ed ha redatto un vademecum: *Deepfake. Il falso che ti "ruba" la faccia (e la privacy)*. E nel 2021 è stata presentata una proposta di legge volta a contrastare proprio l'utilizzo del software "Deepnude" e il revenge porn. **L'obiettivo è quello d'introdurre nel Codice l'illecito della diffusione di immagini manipolate artificialmente allo scopo di ottenerne rappresentazioni nude»**, dice Antonucci. «Oggi l'atto di pubblicare immagini o video sessualmente espliciti senza il consenso delle persone rientra nel reato del revenge porn. Probabilmente uno dei rimedi potrebbe essere limitare la pubblicazione di contenuti che ci riguardano, oppure utilizzare la modalità privata delle piattaforme, ma in un mondo che ci vuole social, diventa una vera sfida». ■

Quando l'Intelligenza artificiale è utile

Ci sono anche grandi vantaggi con l'Intelligenza artificiale che crea i deepfake. Come **il video in cui il sindaco di Venezia Luigi Brugnaro spiega in inglese** come funzionerà il ticket per entrare nella città veneta. Lui stesso ha ammesso di essersi servito di un programma avanzato che ha "copiato" la sua voce e l'ha usata per trasmettere il messaggio in un'altra lingua. La stessa tecnologia che può essere usata per creare video falsi o di satira ha permesso di comunicare meglio.