PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4850 di Venerdì 15 gennaio 2021

Una scheda informativa sui rischi del deepfake

Il Garante per la protezione dei dati personali ha messo a punto una scheda informativa per sensibilizzare gli utenti sui rischi connessi agli usi malevoli di questa nuova tecnologia.

I deepfake sono foto, video e audio creati grazie a software di intelligenza artificiale (AI) che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce.

Il Garante per la protezione dei dati personali ha messo a punto una scheda informativa per sensibilizzare gli utenti sui rischi connessi agli usi malevoli di questa nuova tecnologia, sempre più frequenti, anche a causa della diffusione di app e software che rendono possibile realizzare deepfake, anche molto ben elaborati e sofisticati, utilizzando un comune smartphone.

Cosa è un deepfake?

I deepfake sono foto, video e audio creati grazie a software di intelligenza artificiale (AI) che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce.

La parola deepfake è un neologismo nato dalla fusione dei termini "fake" (falso) e "deep learning", una particolare tecnologia AI. Le tecniche usate dai deepfake sono simili a quelle delle varie app con cui ci si può divertire a modificare la morfologia del volto, a invecchiarlo, a fargli cambiare sesso, ecc. La materia di partenza sono sempre i veri volti, i veri corpi e le vere voci delle persone, trasformati però in "falsi" digitali.

Le tecnologie deepfake, sviluppate come ausilio agli effetti speciali cinematografici, erano inizialmente molto costose e poco diffuse.
Ma negli ultimi tempi hanno iniziato a diffondersi app e software che rendono possibile realizzare deepfake, anche molto ben elaborati e sofisticati, utilizzando un comune smartphone. La diffusione dei deepfake è di conseguenza notevolmente aumentata, e con essa i rischi connessi.

Il deepfake e il furto di identità

Quella realizzata con i deepfake è una forma particolarmente grave di furto di identità.

Le persone che compaiono in un deepfake a loro insaputa non solo subiscono una perdita di controllo sulla loro immagine, ma sono private anche del controllo sulle loro idee e sui loro pensieri, che possono essere travisati in base ai discorsi e ai comportamenti falsi che esprimono nei video.

Le persone presenti nei deepfake potrebbero inoltre essere rappresentate in luoghi o contesti o con persone che non hanno mai frequentato o che non frequenterebbero mai, oppure in situazioni che potrebbero apparire compromettenti.

In sostanza, quindi, un deepfake può ricostruire contesti e situazioni mai effettivamente avvenuti e, se ciò non è voluto dai diretti interessati, può rappresentare una grave minaccia per la riservatezza e la dignità delle persone.

I gravissimi rischi del deepnude

In particolari tipologie di deepfake, dette deepnude, persone ignare possono essere rappresentate nude, in pose discinte, situazioni compromettenti (ad esempio, a letto con presunti amanti) o addirittura in contesti pornografici. Con la tecnologia del deepnude, infatti, i visi delle persone (compresi soggetti minori) possono essere "innestati", utilizzando appositi software, sui corpi di altri soggetti, nudi o impegnati in pose o atti di natura esplicitamente sessuale. E' anche possibile prendere immagini di corpi vestiti e "spogliarli", ricostruendo l'aspetto che avrebbe il corpo sotto gli indumenti e creando immagini altamente realistiche.

Inizialmente il fenomeno ha coinvolto personaggi famosi allo scopo di screditarli o ricattarli. Ma negli ultimi tempi, con la sempre maggiore diffusione di software che utilizzano questa tecnologia, il rischio coinvolge anche persone comuni, le quali possono diventare oggetto di azioni psicologicamente e socialmente molto dannose. Come, ad esempio, il "revenge porn", cioè la condivisione online - a scopo di ricatto, denigrazione o vendetta, da parte di ex partner, amanti o spasimanti respinti - di foto e video a contenuto sessuale o addirittura pornografico, che, nel caso del deepnude, sono ovviamente falsi.

Video deepnude possono essere utilizzati, a totale insaputa dei soggetti rappresentati nelle immagini, anche per alimentare la pratica del sexting (cioè lo scambio e diffusione di immagini di nudo, che a volte coinvolge anche soggetti minori), la pornografia illegale e, purtroppo, anche reati gravissimi come la pedopornografia.

Deepfake e cyberbullismo

I video deepfake possono essere creati ad hoc per realizzare veri e propri atti di cyberbullismo, che hanno come vittime soprattutto giovani.

Un deepfake può essere realizzato per denigrare, irridere e screditare le persone coinvolte, o addirittura per ricattarle, chiedendo soldi o altro in cambio della mancata diffusione del video oppure per la sua cancellazione se è già stato diffuso.

Deepfake e fake news

I deepfake possono riguardare politici o opinion leader, con lo scopo di influenzare l'opinione pubblica. Video deepfake possono ad esempio essere mostrati o inviati agli elettori che simpatizzano per un determinato personaggio politico, rappresentandolo mentre compie azioni poco lecite o mentre si trova in situazioni sconvenienti, allo scopo di screditarlo ed influenzare le opinioni o il voto. In questo modo, i deepfake possono purtroppo contribuire alla diffusione di fake news e alla disinformazione.

Il deepfake può quindi arrivare a privare le persone della cosiddetta "autodeterminazione informativa" ("ciò che voglio far sapere di me lo decido io"), come pure ad incidere sulla loro libertà decisionale ("quello che penso e faccio è una scelta su cui gli altri non possono interferire").

Deepfake e cybercrime

Il deepfake può essere utilizzato per attività telematiche illecite, come lo spoofing (il furto di informazioni che avviene attraverso la falsificazione di identità di persone o dispositivo, in modo da ingannare altre persone o dispositivi e ottenere la trasmissione di dati), il phishing e il ransomware.

Volti e voci artefatti possono essere utilizzati per ingannare i sistemi di sicurezza basati su dati biometrici vocali e facciali. Ad esempio, video o audio-messaggi deepfake creati da malintenzionati possono essere inviati ai nostri colleghi, amici o parenti per invitarli a cliccare su link o aprire allegati a messaggi che espongono pc, smartphone o altri dispositivi e sistemi a

pericolose intrusioni, oppure per convincerli a fornire, ingannando la loro fiducia, informazioni e dati sensibili. Inoltre oggi molti sistemi digitali (domotica, assistenti vocali, smartphone, nonché alcuni sistemi bancari o sanitari) ricorrono a dati biometrici vocali e facciali come sistema di autenticazione per l'accesso. Video e audio-messaggi deepfake potrebbero essere utilizzati per ingannare tali sistemi.

Anche se al momento il livello avanzato delle tecnologie di sicurezza e la ancora relativa imprecisione dei deepfake stanno limitando questi fenomeni, l'attenzione deve essere comunque alta.

Come proteggersi dai deepfake

Le grandi imprese del digitale (piattaforme social media, motori di ricerca, ecc.) stanno già studiando e applicando delle metodologie per il contrasto al fenomeno, come algoritmi di intelligenza artificiale capaci di individuare i deepfake o sistemi per le segnalazioni da parte degli utenti, e stanno formando team specializzati nel monitoraggio e contrasto al deepfake. E le Autorità di protezione dei dati personali possono intervenire per prevenire e sanzionare le violazioni della normativa in materia di protezione dati.

Tuttavia, il primo e più efficace strumento di difesa è rappresentato sempre dalla responsabilità e dall'attenzione degli utenti. Ecco allora alcuni suggerimenti:

- Evitare di diffondere in modo incontrollato immagini personali o dei propri cari. In particolare, se si postano immagini sui social media, è bene ricordare che le stesse potrebbero rimanere online per sempre o che, anche nel caso in cui si decida poi di cancellarle, qualcuno potrebbe già essersene appropriato.
- Anche se non è semplice, si può imparare a riconoscere un deepfake. Ci sono elementi che aiutano: l'immagine può appare pixellata (cioè un pò "sgranata" o sfocata); gli occhi delle persone possono muoversi a volte in modo innaturale; la bocca può apparire deformata o troppo grande mentre la persona dice alcune cose; la luce e le ombre sul viso possono apparire anormali.
- Se si ha il dubbio che un video o un audio siano un deepfake realizzato all'insaputa dell'interessato, occorre assolutamente evitare di condividerlo (per non moltiplicare il danno alle persone con la sua diffusione incontrollata). E si può magari decidere di segnalarlo come possibile falso alla piattaforma che lo ospita (ad esempio, un social media).
- Se si ritiene che il deepfake sia stato utilizzato in modo da compiere un reato o una violazione della privacy, ci si può rivolgere, a seconda dei casi, alle autorità di polizia (ad esempio, alla Polizia postale) o al Garante per la protezione dei dati personali.

Scarica la Scheda informativa " Deepfake Il falso che ti «ruba» la faccia (e la privacy)" (pdf)

Fonte: Garante Privacy