Riconoscimento facciale, dopo 40 anni di ricerche fa ancora paura. Il report

Dopo 40 anni di studi, i ricercatori hanno ammesso che il riconoscimento facciale è diventato uno strumento di sorveglianza sempre più potente attraverso il quale l'ultima generazione della tecnologia, quella basata sul **deep learning**, ha completamente sconvolto le norme di consenso per la privacy.

Lo rivela lo studio ***"About Face: A Survey of Facial Recognition Evaluation"*** condotto da due ricercatrici **Deborah Raji,** una ricercatrice dell'organizzazione no profit **Mozilla**, e **Genevieve Fried,** consigliere dei membri del Congresso degli Stati Uniti sulla responsabilità algoritmica. Le due ricercatrici hanno esaminato oltre 130 set di dati sul riconoscimento facciale compilati in 43 anni.

La ricerca, ripresa da Tecnologyreview.com, la rivista scientifica di proprietà del **Massachusetts Institute of Technology** (MIT), ha evidenziato come la scienza, spinta dall'esplosione dei requisiti di dati del Deep Learning, ha gradualmente abbandonato la richiesta del consenso portando a incorporare sempre più foto personali delle persone in sistemi di sorveglianza, a loro insaputa.

La storia del riconoscimento facciale

I ricercatori erano estremamente cauti nel raccogliere, documentare e verificare i dati sui volti nei primi anni 90, dice Raji. "*Adesso non ci interessa più. Tutto questo è stato abbandonato* ", spiega a Tecnologyreview.com.

Le due ricartrici hanno identificato quattro epoche principali del riconoscimento facciale, ciascuna guidata da un crescente desiderio di migliorare la tecnologia. La prima fase, che durò fino agli anni ’90, era in gran parte caratterizzata da metodi manuali e lenti dal punto di vista computazionale.

Sebbene gli sforzi per sviluppare il riconoscimento facciale siano iniziati in ambienti accademici, la svolta si ebbe nel 1996 quando il Dipartimento della Difesa degli Stati Uniti e il National Institute of Standards and Technology (**NIST**) hanno stanziato 6,5 milioni di dollari per creare il più grande set di dati fino ad oggi.

“Il decennio successivo ha visto un aumento della ricerca accademica e commerciale sul riconoscimento facciale e sono

stati creati molti altri set di dati”, spiegano le ricercatrici. La stragrande maggioranza proveniva da servizi fotografici come FERET e aveva il pieno consenso dei partecipanti. *“Molti includevano anche metadati meticolosi”,* dice Raji, come l’età e l’etnia dei soggetti o le informazioni sull’illuminazione.

Nel 2007, il rilascio del set di dati **Labeled Faces in the Wild** (LFW), ha aperto le porte alla raccolta di dati tramite la ricerca sul web. I ricercatori hanno iniziato a scaricare immagini direttamente da **Google**, **Flickr** e **Yahoo** senza preoccuparsi del consenso. LFW ha anche abbassato gli standard sull’inclusione dei minori, utilizzando foto trovate con termini di ricerca come “bambino”, “giovanile” e “adolescente” per aumentare la diversità. Questo processo ha permesso di creare set di dati significativamente più grandi in breve tempo, ma il riconoscimento facciale ha comunque dovuto affrontare molte delle stesse sfide di prima. Ciò ha spinto i ricercatori a cercare ancora più metodi e dati per superare le scarse prestazioni della tecnologia.

Il boom successivo del riconoscimento facciale è arrivato da Facebook

I ricercatori citano un punto di svolta nel riconoscimento facciale quando **Facebook** ha rivelato la creazione del suo database **DeepFace** nel 2014. Il social, ha mostrato come la raccolta di milioni di foto potrebbe creare reti neurali che erano di gran lunga migliori nei compiti di riconoscimento facciale rispetto ai sistemi precedenti, rendendo il *deep learning* un pietra angolare del moderno riconoscimento facciale.

Facebook da allora è stato multato dalla FTC per aver utilizzato le foto caricate dagli utenti e per aver consentito il riconoscimento facciale senza chiedere il consenso .

Amba Kak, direttore delle politiche globali di **AI Now**, che non ha partecipato alla ricerca, ha affermato che il documento offre un quadro netto di come si è evoluta l'industria biometrica. *"Il deep learning potrebbe aver salvato la tecnologia da alcune delle sue difficoltà*, ha affermato a Tecnologyreview.com, *"ma questo progresso tecnologico ha avuto un costo: consenso, estrazione, problemi di proprietà intellettuale, privacy."*

Col deep learning la privacy non esiste più

Raji ha dichiarato che la sua indagine sui dati, l'ha resa seriamente preoccupata per il riconoscimento facciale basato sul deep learning.

"È molto più pericoloso", ha spiegato nel report. *"Il requisito dei dati ti costringe a raccogliere informazioni incredibilmente sensibili su, almeno, decine di migliaia di persone. Ti costringe a violare la loro privacy. Questo di per sé è una base del danno. E poi stiamo accumulando tutte queste informazioni che non puoi controllare per costruire qualcosa che probabilmente funzionerà in modi che non puoi nemmeno prevedere".*

Spera che il documento induca i ricercatori a riflettere sul compromesso tra i guadagni in termini di prestazioni derivati dal deep learning e la perdita del consenso, una meticolosa verifica dei dati e una documentazione completa.

Esorta coloro che vogliono continuare a costruire il riconoscimento facciale a prendere in considerazione lo sviluppo di tecniche diverse: *"Per noi provare davvero a usare*

questo strumento senza ferire le persone richiederà di rivedere tutto ciò che sappiamo al riguardo.

Per approfondire

https://www.key4biz.it/riconoscimento-facciale-dopo-40-anni-di-ricerche-fa-ancora-paura-il-report/343708/