IL FALSO MITO DELLE IMPRONTE DIGITALI

Si è sempre ritenuto che i segni lasciati dai polpastrelli fossero esclusivi per ogni dito (e in ogni persona). Ora uno studio basato sull'Intelligenza artificiale dimostra che così non è. E questo potrebbe modificare molte indagini forensi sulla ricerca dei colpevoli di un crimine.

di Luca Sciortino

Le impronte digitali sono cruciali per il funzionamento della società. Sono parte integrante dei nostri sistemi di autenticazione, dai cellulari ai computer, dai sistemi di sicurezza alle porte e ai cancelli, oltre a costituire lo strumento principe delle indagini giudiziarie. Tutto questo perché riteniamo che l'impronta di un dito sia unica: nessun'altro ce l'ha. Ma è davvero così? L'intelligenza artificiale sta sfatando il mito della loro unicità mettendo in dubbio una serie di assunti che ritenevamo dogmaticamente veri.

L'ultimo colpo arriva da una pubblicazione su *Science Advances* di un gruppo di ingegneri della Columbia University. Usando l'Ia, i ricercatori hanno dimostrato che le impronte digitali di differenti dita della stessa persona non sono così distinte tra loro ma hanno qualcosa sempre in comune (possono arrivare ad avere numerose analogie). E questo smentisce un assunto ritenuto sacro nelle indagini forensi. Gli investigatori usano le tracce lasciate dai polpastrelli per attribuire la colpa di un delitto a un criminale; ma se quest'ultimo lascia impronte di differenti dita in due diverse scene del crimine, allora i due delitti difficilmente possono essere messi in relazione. Significa che i colpevoli possono farla franca e talvolta che innocenti vengono messi sotto processo ingiustamente.

Ciò che hanno fatto gli ingegneri americani è stato istruire un sistema basato sugli algoritmi con 60 mila impronte digitali prelevate da una banca dati del governo. Contrariamente a quanto ritenuto, è emerso che - con il 99,9 per cento di affidabilità - ci sono sempre similarità tra impronte digitali della stessa persona. In molti si chiederanno come mai l'intelligenza artificiale sia stata capace di ribaltare decine di anni di analisi. «Il fatto è che il nostro sistema di Ia non si è basato su certi dettagli, tecnicamente chiamati "minutiae", quali le diramazioni o le terminazioni delle creste nell'impronta, come è accaduto finora negli studi tradizionali» dice Gabe Guo, uno degli autori della ricerca. «Ci ha invece permesso di fare qualcosa di diverso: ci siamo concentrati sugli angoli e le curvature delle spirali al centro della traccia. Man mano che aumenta il numero delle impronte digitali con cui si istruisce l'algoritmo, ci si rende conto che il nostro risultato è corretto».

Conclusione di per sé notevole perché mostra come l'Ia abbia le potenzialità di sovvertire idee radicate nel tempo e non sia un puro gioco di rimasticamento di vecchie conoscenze.

E se le impronte digitali appartenessero a dita di due diverse persone? Va messo in chiaro che l'ipotesi dell'unicità è stata sempre ritenuta vera solo sulla base dei risultati empirici. Non esiste alcuna dimostrazione matematica che stabilisca l'impossibilità di due individui con impronte digitali identiche.

Quello che si può dire è che da quando, nel 1880, lo scienziato scozzese Henry Faulds suggerì su *Nature* di usare la loro presunta esclusività per identificare i colpevoli, non sono mai state trovate impronte uguali appartenenti a soggetti differenti. O, almeno, così sembra. Una recente pubblicazione su *Transaction on Information Forensics and Security* suggerisce che le impronte digitali di individui diversi hanno in comune alcune caratteristiche. Basandosi su questi tratti, sarebbe in principio possibile, per i criminali, costruire un passepartout sintetico per le impronte digitali, in gomma o silicone, valido per un significativo numero di casi e capace di ingannare i sistemi di autenticazione.

Impronte di dita diverse sono riconducibili alla stessa persona: e l'Intelligenza artificiale indovina con un'accuratezza che arriva fino al 99,9 per cento.

«Le ultime ricerche mostrano che esiste il rischio per i sistemi di autenticazione parziali, basati su più impressioni per dito in varie posizioni, come quelle per registrare la nostra impronta su un iPhone» aggiunge Guo. «E che sono, almeno potenzialmente, vulnerabili». Di fatto, è noto che al Mobile World Congress del 2016, manifestazione dedicata al commercio della comunicazione via dispositivi mobili, il sistema di autenticazione di un iPhone fu ingannato con un'impronta ricalcata nel pongo.

Un altro studio su *Cell* suggerisce che le peculiarità di un'impronta digitale sarebbero determinate dai geni: sono definitivamente formate alla nascita e non si modificano nel caso di graffi o di tagli. Insomma, quelle che abbiamo dobbiamo tenercele. Meglio allora custodirne gelosamente le caratteristiche, visti i progressi dell'intelligenza artificiale e la possibilità di replicarle.

Sempre che non vogliamo modificarle chirurgicamente. Ma anche così occorre sapere che, nel caso di un'indagine, un medico sarebbe in grado di notare che la nostra impronta non è poi tanto originale dato che al posto di una «cresta» ci sarebbe una cicatrice. ■

iStock