Qui si rischia la faccia

Sono vent'anni che si usano i computer per il riconoscimento facciale ma oggi l'incrocio dati-immagini realizzato dai social media mette a rischio le nostre vite digitale e reale

di **Patrizia Caraveo**

In quanti modi è possibile identificare in modo univoco una persona? Il commissario Maigret non avrebbe avuto dubbi: le impronte digitali, una caratteristica unica, facilmente rivelabile, diversa per ogni essere umano, che lo accompagna immutabile per tutta la vita. James Bond, più tecnologicamente avanzato, in *Mai dire mai* usa il riconoscimento dell'iride, ovviamente da parte di un calcolatore, per penetrare in ambiente top secret. Allora era fantasia, ma oggi è una misurazione biometrica facilmente utilizzabile. Anche la grafia di una persona è un tratto caratteristico e le perizie calligrafiche continuano ad avere un loro utilizzo nelle aule dei tribunali. Tuttavia, l'utilizzo di mail, sms, social media sta facendo perdere la consuetudine alla scrittura manuale, diminuendo l'interesse alla grafia come mezzo di identificazione. Nelle cronache giudiziarie sentiamo sempre più spesso parlare di analisi del Dna, il codice genetico presente in ognuna delle nostre cellule che è inequivocabilmente legato a ciascuno di noi e che porta scritta la storia dei nostri antenati e, in parte, il nostro futuro perché nei geni si può leggere la propensione a un consistente numero di malattie.

Tuttavia, noi non abbiamo bisogno né delle impronte digitali, né dello studio dell'iride, né della mappatura del codice genetico per riconoscere i nostri amici. Ci basta guardarli in faccia, oppure ascoltare la loro voce. Possiamo tranquillamente fare a meno della loro presenza fisica, il riconoscimento può essere facilmente fatto attraverso una foto, un filmato o semplicemente un audio. Ovviamente, nessuno di noi si preoccupa di essere riconosciuto dalla sua cerchia di amici, conoscenti e collaboratori, quasi tutti, però, troverebbero per lo meno sgradevole essere facilmente identificabili da perfetti sconosciuti, grazie a programmi di riconoscimento facciale o vocale. È quello che potrebbe avvenire, e in parte già avviene, sfruttando una zona grigia della legislazione sulla privacy che non tutela la nostra faccia o la nostra voce. Il riconoscimento facciale (e vocale) è un interessante esempio di un'area dove l'avanzamento tecnologico corre molto più velocemente della normativa che dovrebbe regolarne l'uso.

È da circa vent'anni che i computer sanno riconoscere la presenza di un volto in un'immagine. I tratti salienti sono sempre gli stessi: due occhi, due orecchie, un naso, una bocca con delle posizioni relative più o meno fissate. Invece, per dare un nome al volto occorre poterlo sovrapporre in modo soddisfacente con altre foto della stessa persona magari fatte in altre pose, con diversa illuminazione, un diverso look, una diversa pettinatura, ad anni di distanza. Identificare è molto più difficile che riconoscere e ha richiesto anni di sforzi e di ingenti investimenti per mettere a punto procedure di *deep learning* basate su una galleria di immagini, generalmente personaggi pubblici, ripresi in momenti e in atteggiamenti diversi, sui quali mettere alla prova i programmi, fino ad arrivare a ottenere risultati soddisfacenti. Alla fine, un viso viene schematizzato con una griglia codificata con appena 256 bit, un'inezia informatica. È quello che si chiama *faceprint*, l'impronta della nostra faccia, la versione moderna della maschera mortuaria dei grandi del passato. *Faceprint* non è un'immagine ma una griglia di punti ed è la base dei programmi di riconoscimento facciale veloce.

SORVEGLIATI | *John Reese, ex agente della Cia e Harold Finch (di profilo), miliardario appassionato di computer, sono i protagonisti della serie tv «Person of Interest», 2011*

Mentre è evidente che la polizia ha sempre fatto uso di software di riconoscimento facciale per individuare i criminali già schedati, estrarre un volto dalla folla, localizzare e seguire sospetti che entrano ed escono dal campo delle telecamere di sorveglianza, le persone normali non pensano di meritarsi questo trattamento. Il campanello d'allarme è suonato quando è trapelata la notizia che, in vista dell'uscita dei Google Glass, FacialNetwork era pronta a mettere sul mercato l'applicazione *NameTag*. Sarebbe bastata una foto fatta da google Glass, per risalire in meno di un secondo a nome e professione, corredate da notizie estratte dai social media, di (quasi) ogni persona incontrata per strada, senza che questa ne fosse minimamente informata. Una evidente violazione della privacy. A seguito della sollevazione popolare, Google ha giurato che non avrebbe autorizzato *NameTag* sui Google Glass, che, peraltro, hanno ancora un sacco di problemi e sembrano essere stati congelati dai loro sviluppatori. Parallelamente, Facebook diffidava *NameTag* dall'usare la sua sterminata galleria di foto, per la quale aveva in mente un altro utilizzo, sempre di riconoscimento facciale, ma declinato in difesa della privacy. Facebook, infatti, pianifica di utilizzare *DeepFace*, il suo software di riconoscimento facciale, per proteggere la privacy dei suoi 1,3 miliardi di utenti. La posta in gioco è alta e *DeepFace* è straordinariamente accurato: sbaglia nel 2% dei casi, come un umano. Ogni volta che viene postata una nuova foto (e succede quattrocento milioni di volte al giorno), *DeepFace* riconosce i componenti dell'allegra brigata e, se ci siete anche voi, vi avvisa e vi chiede se siete d'accordo ad essere riconoscibile nella foto oppure se preferite che il vostro viso venga sfuocato, per restare anonimo. Un gentile pensiero che dimostra che tutti gli utenti di Facebook sono "*faceprinted*", cioè riconoscibili.

Mentre ciascuno di noi può decidere di avere il suo viso *faceprinted* per poi usarlo come password omnicomprensiva di tutti i suoi account, come chiave di casa, del conto in banca, e per evitare code alla sicurezza degli aeroporti, essere *faceprinted* a nostra insaputa è cosa ben diversa, e molto più preoccupante.

Ovviamente, si può obbiettare che siamo noi stessi a mettere online le foto e le informazioni dalle quali attingono questi sistemi... Indietro non si torna. Per tutelare la nostra vita digitale (e reale) occorre agire in fretta: nessuno si può separare dalla propria faccia e neppure dalla propria voce.