Riconoscimento facciale e sorveglianza: raising awareness

di Federica Paolucci

Il riconoscimento facciale è una tecnologia a base biometrica che raccoglie e processa immagini digitali che riproducono volti di individui allo scopo di identificazione, autenticazione o verifica, categorizzazione e classificazione degli stessi[1]. Dal punto di vista tecnico può essere definito un network neurale "multi-layered". Come indicato da Norbert Wiener[2], matematico e padre della cibernetica, questo sistema consente a una formula matematica di funzionare come un cervello umano e procede, dunque, a una corretta analisi e *match* a seguito e tramite l'accumulo di una grande quantitativo di dati ed informazioni.

Dal punto di vista, invece, prettamente sociale il riconoscimento facciale può essere identificato come un (ulteriore) invasivo strumento di sorveglianza che ha delle gravi ripercussioni sull'esercizio delle libertà individuali. Con un'efficace frase, sebbene iperbolica, l'artista e attivista Adam Harvey afferma che «il selfie di oggi è l'attività biometrica di domani»: anche le foto che vengono caricate sui profili social sono sottoposte a un'incessante attività di analisi in grado di estrapolare dati relativi ai nostri volti per consentire all'algoritmo di individuare e raccogliere quelli definiti dalle fonti europee come *«special categories of personal data»*, ossia dati che riguardano aspetti intrinsecamente connessi alla personalità umana (ad esempio, dati etnici, raziali o di genere, relativi allo stato di salute o all'orientamento sessuale).

Dal punto di vista giuridico, il riconoscimento facciale non è oggetto di nessuna specifica normativa se non dei limiti posti dal GDPR per i dati biometrici. Difatti, nell'art. 9 si specificano in negativo, al par. 2, le aree in cui può essere effettuato il trattamento di tali dati: quali, ad esempio, finalità specifiche relative alla sicurezza degli individui. Dal punto di vista regolatorio, occorre prendere atto del fatto che già lo scorso gennaio, durante le consultazioni che hanno preceduto l'adozione del White Paper on Artificial Intelligence, nel febbraio del 2020, – prima che l'emergenza provocata dal virus SARS-COV-2 diventasse la massima urgenza nelle agende politiche dell'intero globo – la Commissione Europea stava considerando la possibilità di istituire un *moratorium* di cinque anni con ad oggetto proprio l'uso del Facial Recognition Technology (FRT) negli spazi aperti al pubblico. Una misura che da ultimo non è stata adottata, lasciando ancora una volta in sospeso un gran numero di questioni relative al suo legittimo utilizzo nella cornice del diritto eurounitario. Un'assenza che non è stata colmata nemmeno dalle generiche Linee Guida pubblicate nel gennaio 2021 dal CoE[3]. Un'inversione di rotta sembra essere, invece, quella perseguita dalla Commissione nella Proposta di Regolamento sull'Intelligenza Artificiale dove all'art. 5 classifica l'uso di *real time remote biometric identification* per attività di *law enforcement* (tra cui il riconoscimento facciale) come "da proibire". Si deve chiarire però che non si tratta di un *ban* totale del riconoscimento

facciale in quanto la stessa bozza di norma prevede diverse eccezioni e non ricomprende tutti quegli usi non “live” della tecnologia, come nel caso di immagini già raccolte.

Tralasciando gli aspetti giuridici legati al riconoscimento facciale, la domanda a cui occorre rispondere per consentire una comprensione del fenomeno è: le nostre vite sono effettivamente toccate da questa misteriosa tecnologia? La risposta è affermativa. Chiunque possieda uno *smartphone* di ultima generazione, può utilizzare la biometria per sbloccarlo (che sia il Face ID in uso già da diversi anni da Apple o anche la semplice raccolta dell’impronta digitale). Chiunque abbia un account su Facebook e ha caricato le proprie foto sul social o sia stato “taggato” dai propri contatti in qualche immagine raffigurante visi, è stato oggetto di analisi facciale. Come? Lo spiega lo stesso social network: si crea un “modello” del volto e lo si usa per confrontarlo con altre foto, video e altri elementi digitali nei quali viene usata la fotocamera, come nelle dirette.

Inoltre, il riconoscimento facciale non è solo prerogativa dei privati: una delle sue più famose applicazioni è un database creato da un’azienda statunitense, Clearview AI. Tale archivio contiene migliaia di volti ricavati da fotografie “pubbliche”, ossia pubblicate su siti web tra cui social network come Facebook, o ancora foto da albi o eventi divulgate online. Questo *database* viene utilizzato dalla polizia per rintracciare sospetti: sempre a partire da un “modello”, si confrontano le foto da analizzare con quelle presenti nel database per rintracciare l’identità di un individuo. Se già di per sé l’idea che foto di individui inconsapevoli vengano utilizzate come *training* di un algoritmo è alquanto preoccupante; il fatto poi che tale tecnologia produca dei (*coded*) *bias* (errori nella corretta identificazione di alcuni individui e che possono amplificare forme di discriminazione razziale, di genere, abilismo) per citare il documentario di recente diffuso da Netflix, la rende pericolosa e inutilmente intrusiva. Per questa ragione, molti stati (ad esempio il Canada) che la stavano applicando si stanno muovendo verso un blocco di Clearview, in quanto se ne stanno apprezzando le criticità dal punto di vista sociale e giuridico.

Un caso emblematico ha riguardato l’installazione di telecamere programmate fornite dalla azienda Cisco a due scuole del Sud della Francia. Gli studenti (minori) sono stati oggetto di un progetto sperimentale basato su riconoscimento facciale: una vicenda che si è conclusa con un’importante pronuncia del Tribunale Amministrativo di Marsiglia ove si è stabilito che l’installazione di tali telecamere rappresentava una violazione dei diritti fondamentali degli studenti, contraria al principio di proporzionalità previsto dal GDPR, e che privava inoltre gli studenti della possibilità di esprimere un consenso libero a causa dello squilibrio di potere tra interessati (gli studenti appunto) e titolare del trattamento (la scuola).

Siamo, dunque, al cospetto di una tecnologia in grado di effettuare una sorveglianza di tipo massivo su minori e adulti che preoccupa per il suo grado di invasività e per i c.d. *chilling effects* che può produrre nell’esercizio delle libertà fondamentali (ad esempio,

di tipo associativo) simbolo ed espressione di una società che vuole definirsi democratica. Una preoccupazione tutt'altro che utopica o distopica, ma che anzi colpisce da vicino l'Italia ove è in uso, da parte della polizia, un database chiamato SARI[4] sul quale si è recentemente espressa l'Autorità Garante fornendo al Ministero dell'Interno un parere negativo circa l'utilizzabilità del sistema.

È, dunque, di vitale importanza parlare degli utilizzi del riconoscimento facciale[5] coinvolgendo attivamente gli individui che, spesso non consapevolmente, sono oggetto di queste analisi. Stanno nascendo diverse campagne sull'argomento: una su tutte, quella lanciata dal centro European Citizens' Initiative, "Reclaim your Face", che ha lo scopo di sensibilizzare sul tema tanto la società civile quanto le istituzioni. Alcune delle maggiori *corporation* hanno già fatto dei passi indietro date le conseguenze sociali che una tale tecnologia può provocar, come, ad esempio, IBM. Al motto di "ridateci la faccia" non possiamo far altro che informare ed informarci sui rischi correlati a tale tecnologia e sperare che le istituzioni europee prendano presto una posizione: non un passo indietro dal punto di vista tecnico-digitale, ma una necessaria e urgente riflessione che deve essere il naturale percorso per evitare eccessive e sproporzionate invasioni nella privacy degli individui.

[1] Definizione dell'*Article 29 Data Protection Working Party* (2012), Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN, WP 192, Bruxel, 22 Marzo 2012, p. 2.

[2] Norbert Wiener, *Cybernetics or Control and Communication in the Animal and the Machine* (MIT press, 2019).

[3] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, Convention 108: Guidelines on facial recognition, 28 gennaio 2021.

[4] Si veda sul punto «Come usa la polizia italiana il riconoscimento facciale?», *La Stampa,* consultato 25 febbraio 2021. Meritano un'attenzione particolare le parole di Riccardo Coluccini, Vicepresidente della ONG per i diritti civili in ambito digitale, Hermes Center, sui gravi *bias* (errori) prodotti dal riconoscimento facciale, in particolare, quando deve riconoscere volti di persone di colore. In modo più esteso, su «Riconoscimento

facciale, nel database di Sari quasi 8 schedati su 10 sono stranieri»*Wired* (blog), 3 aprile 2019.

[5] Stanno nascendo diverse campagne sull'argomento. Una su tutte, quella lanciata dal centro European Citizens' Initiative: "Reclaim your Face".