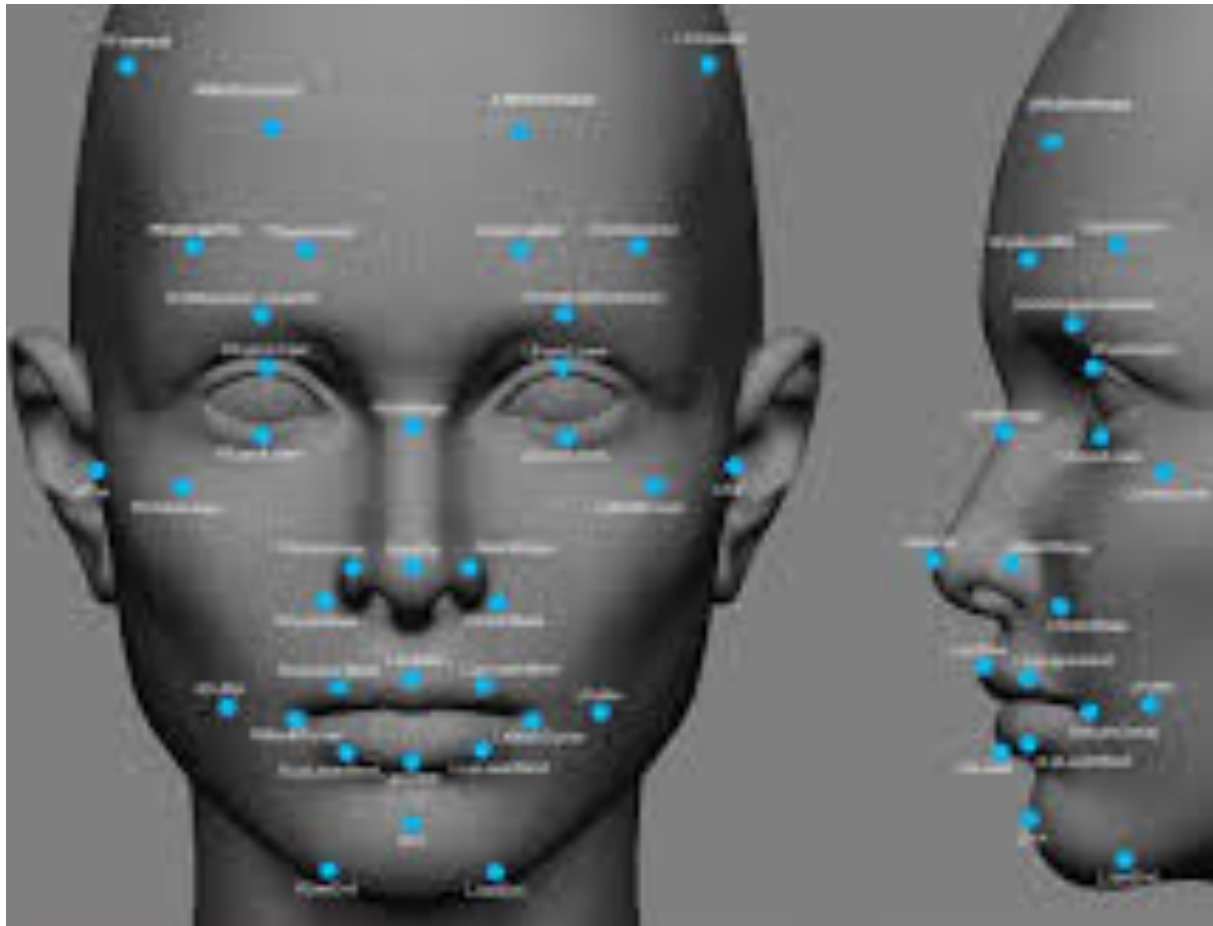




Facial Recognition: tra opportunità e rischi

La rapidità degli scambi e delle transazioni del mondo interconnesso, accompagnata da una crescente necessità di sicurezza, hanno contribuito al vertiginoso sviluppo delle tecnologie basate sui sistemi c.d. biometrici, ovvero tutti quei dispositivi automatici che consentono

“Il valore del mercato del facial recognition aumenterà dagli attuali 3.2 miliardi di dollari (riferito al 2019) a 7 miliardi entro il 2024”

MarketsandMarkets



l'identificazione di una persona attraverso caratteristiche biologiche – sia esse fisiologiche (come l'occhio, il volto, l'impronta, il dna) che comportamentali. Esse rappresentano una delle più grandi risorse – ed allo stesso tempo sfide – tecnologiche (unitamente all'AI e alle blockchain), soprattutto per i soggetti pubblici, per via dei molteplici settori in cui possono essere utilizzate e dei conseguenti vantaggi che possono generare.

Non a caso, paesi in forte espansione come la Cina hanno investito enormi risorse (sia umane che economiche) sullo sviluppo di tali tecnologie, utilizzandole in maniera sempre più ampia al loro interno (come la recente applicazione ai tornelli della metropolitana di Shenzhen per consentire l'accesso a determinate fasce di utenti, ovvero le recenti applicazioni nel settore della zootecnica¹), ed offrendole a prezzi competitivi anche ad altri stati al fine di ottenere in cambio dati di cui servirsi a fini di ricerca e sviluppo².

Le soluzioni messe a punto variano dal “semplice” riconoscimento dell'impronta digitale a quello più accurato della retina, delle vene del dito (c.d. finger-vein technology³), della voce o a quello sempre più diffuso del volto. Proprio quest'ultimo – in ragione della facilità e trasversalità di applicazione – ha visto una crescita esponenziale negli ultimi anni.

Secondo una recente ricerca americana il valore del mercato del facial recognition aumenterà dagli attuali 3.2 miliardi di dollari (riferito al 2019) a 7 miliardi entro il 2024⁴: negli ultimi anni, il settore che ha investito di più su tali tecnologie è stato quello dei servizi finanziari, ma la domanda è in costante crescita nei settori militari, governativi e della sicurezza interna, del retail e della sanità.

“In Cina circa 170 milioni di videocamere intelligenti vengono utilizzate soprattutto dalle forze di polizia per la repressione dei reati”



L'uso più diffuso (e che più sta facendo discutere) è sicuramente quello applicato al campo della sicurezza, per finalità di prevenzione e accertamento dei reati, soprattutto di matrice terroristica (ma non solo): dispositivi di riconoscimento facciale sono sempre più utilizzati negli aeroporti, nelle stazioni o nei luoghi affollati e/o oggetto di grandi eventi, dove software via via più accurati riescono ad acquisire l'immagine di migliaia di volti in pochi secondi per poi confrontarli con quelli contenuti in data-base preesistenti.

Sperimentazioni sono in corso in ben 30 stati USA, così come in UK o in Canada: già nel 2017, in occasione della finale di Champions League a Cardiff, è stato utilizzato un software del genere e altrettanto avverrà per le olimpiadi di Tokyo 2020, per le quali il facial recognition system sarà lo strumento cardine per gestire gli accessi e la sicurezza degli eventi sportivi. Anche in Italia FIGC e Lega Calcio hanno di recente annunciato il ricorso a sistemi di riconoscimento facciale per combattere il fenomeno del razzismo negli stadi⁵, così come numerose società che gestiscono eventi stanno effettuando ingenti investimenti in tecnologie di riconoscimento per la gestione sicura ed efficiente di concerti e grandi spettacoli⁶.

Tuttavia, non mancano le critiche – talvolta anche molto aspre – per gli errori in cui i sistemi ancora incorrono. Tra il 2016 ed il 2019 il Metropolitan Police Service inglese ha condotto 10 test di live facing recognition durante operazioni di polizia volte all'identificazione di persone ritenute sospette: su 42 casi di possibile match individuato dal software, solo 8 sono risultati corretti (il 19.05%)⁷.

Anche negli USA, molte città hanno abbandonato l'uso sperimentale di tali programmi per il controllo del territorio, lamentando l'inattendibilità del riconoscimento ed il rischio di gravi violazioni dei diritti umani: in molti casi, infatti, si sono registrati margini di errore più ampi nei confronti di persone di colore, soprattutto donne⁸.

Eppure, secondo un recente rapporto pubblicato dal NIST (National Institute of Standards and Technology) dello U.S. Department of Commerce, l'accuratezza dei software è aumentata esponenzialmente negli ultimi 5 anni: dall'analisi di ben 127 algoritmi di 45 tra i maggiori produttori, è emerso un margine di errore dello 0,2%, rispetto al 4% registrato nel 2014⁹. Ciò è sicuramente il frutto del potenziamento dell'Intelligenza Artificiale e delle continue evoluzioni nel deep learning, che consentono oggi alle macchine di acquisire nuove competenze, come la capacità di identificare non solo il volto di una persona ma anche i suoi sentimenti o le emozioni che da esso traspaiono.

Oltre alla potenziale violazione di diritti umani, la maggior critica che tali tecnologie sollevano è legata alla protezione dei dati raccolti: come vengono gestiti, conservati e utilizzati? E con quali rischi? Ed infatti, anche nei paesi in cui la privacy gode di una tutela forte e radicata nel tempo, emergono lacune e vuoti legislativi che, in molti casi, conducono a rinunciare alla sfida tecnologica e, conseguentemente, ai benefici potenziali ad essa connessi.

Nel 2016 in Europa è entrato in vigore il GDPR (General Data Protection Regulation), il quale include i dati biometrici tra le "categorie particolari di dati" per i quali è vietato il trattamento a meno che non vi sia esplicito consenso, ovvero ci si trovi in uno degli altri casi tassativamente previsti e disciplinati dall'art. 9¹⁰. Tale cornice normativa trova diretta applicazione in tutti i paesi dell'Unione Europea e rispetto a tutti i soggetti che operino al suo interno (a prescindere dalla loro nazionalità o paese di provenienza).

Negli USA non esiste una normativa federale sulla privacy (ed in particolare sul tema dei dati biometrici), tuttavia agenzie governative e grandi gruppi industriali si sono dotati nel tempo di una serie di guidelines di condotta che sicuramente pongono le basi per una futura regulation generale: gli stati di Washington, Illinois e Texas hanno approvato nel 2017 leggi specifiche in tema di biometric privacy e molti

altri stati stanno predisponendo normative simili e sempre più dettagliate¹¹.

Un cenno a parte merita invece la California, dove a giugno del 2018 è stato approvato il CCPA (California Consumer Privacy Act), il quale disciplina in maniera stringente la privacy a tutela soprattutto dei consumatori: non a caso, città come San Francisco e Oakland (seguite poi dalla città di Somerville nel Massachusetts) a maggio del 2019 hanno vietato l'uso del facial recognition da parte delle forze di polizia ed altre agenzie governative¹², a causa dei rischi concreti per i diritti e le libertà civili dei cittadini che tali sistemi comportano. Una scelta sicuramente singolare – ma forse prevedibile – per la patria delle Big Tech della Silicon Valley (Amazon, Facebook, Google etc.) che sul facial recognition stanno investendo enormi risorse.

È innegabile, tuttavia, che l'utilizzo di tali sistemi da parte di paesi con scarsa democratizzazione o, peggio, di riconosciuti regimi totalitari, rappresenti un rischio più che concreto per la libertà e gli altri diritti fondamentali. Basti pensare alle recenti tensioni di Hong Kong, dove i manifestanti hanno deciso di celare il proprio volto per evitare di essere identificati dai c.d. “pali della luce intelligenti” (perché dotati di videocamere integrate con software di riconoscimento facciale), oppure in Cina, dove l'utilizzo massivo del riconoscimento facciale ha creato un vero e proprio “stato di sorveglianza globale”, con circa 170 milioni di videocamere intelligenti utilizzate soprattutto dalle forze di polizia per la repressione dei reati¹³.

Al netto delle critiche, in ogni caso, non bisogna sottovalutare i potenziali vantaggi che tecnologie del genere potrebbero arrecare in settori quali la salute, la giustizia o, perfino, la gestione di processi democratici fondamentali come le elezioni: il Brasile, ad esempio, ha annunciato l'intenzione di censire tutti i cittadini del paese entro il 2020 e creare un sistema di identità elettroniche, attraverso la raccolta di dati biometrici da parte del TSE (Tribunal Superior Eleitoral), soprattutto al fine di evitare le frodi elettorali. Il facial recognition, dunque, potrebbe essere un utile alleato per i sistemi di voto elettronico che, ancora oggi, stentano a diffondersi per via della loro non totale affidabilità.

Ancora una volta, pertanto, il tema delle tecnologie cyber pone l'esigenza di una regolamentazione generale che riesca a contemperare le esigenze di tutela e rispetto dei diritti umani, con quelle di una maggiore sicurezza: sarà compito di tutti gli attori coinvolti (dagli Stati alle grandi aziende, fino ai singoli cittadini) partecipare attivamente alla loro realizzazione.

¹ Guido Romeo “Il riconoscimento facciale salverà i maiali (ma anche le vacche)”, Il Sole 24Ore, 9.06.2019.

² <https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/>

³ Un uso sempre più ampio della tecnologia del finger-vein, si ha soprattutto nel campo della salute, per via della sua scarsa invasività e dell’alta percentuale di sicurezza: cfr. Jim Canham - *Biometrics: leap of faith or fact of life?* - Biometric Technology Today, Volume 2018, Issue 2, February 2018.

⁴ MarketsandMarkets - Facial Recognition Market by Component (Software, Tools, and Services), Application Area (Emotion Recognition, Attendance Tracking and Monitoring, Access Control, Law Enforcement), Vertical, and Region - Global Forecast to 2024 – June, 2019.

⁵ <https://www.sporteconomy.it/de-siervo-lega-calcio-riconoscimento-facciale-dei-tifosi-negli-stadi-per-contrastare-il-razzismo/> - <https://onefootball.com/it/notizie/idea-figc-riconoscimento-facciale-allo-stadio-per-razzisti-it-27359826?variable=20191009>

⁶ https://www.agi.it/innovazione/concerti_live_nation_riconoscimento_facciale-3861997/news/2018-05-07/

⁷ Independent Report on the London Metropolitan Service’s Trial of Live Facial Recognition Technology – Human Right Center – University of Essex, July 2019.

⁸ M.I.T. Media Lab study “Gender shades” - <https://www.media.mit.edu/projects/gender-shades/overview/>.

⁹ NISTIR 8238 “Ongoing Face Recognition Vendor Test (FRVT), Part II: identification”, November 2018.

¹⁰ Cfr. Art. 4 (dati biometrici e relativi alla salute) e Art. 9 GDPR (categorie particolari di dati), il quale indica tassativamente i casi in cui è possibile trattare tali categorie di dati.

¹¹ “Biometric data and data protection regulations (GDPR and CCPA) - <https://www.gemalto.com/govt/biometrics/biometric-data>

¹² <https://www.nytimes.com/2019/07/01/us/facial-recognition-san-francisco.html>

¹³ <https://www.agendadigitale.eu/sicurezza/privacy/riconoscimento-facciale-e-allarme-privacy-nel-mondo-ecco-i-rischi-e-le-misure-a-tutela/>