CENTRO STUDI INTERNAZIONALI

SAFETY, SECURITY, PRIVACY: I DILEMMI PER L'USO DEI DATI BIOMETRICI IN EUROPA

Di Veronica Conti

Aprile 2020

A fine febbraio è trapelato un documento dell'Unione Europea secondo cui le Forze dell'Ordine di 10 Paesi membri, capitanate dalla Polizia austriaca, avrebbero avanzato l'idea di **utilizzare tecnologie per il riconoscimento facciale per creare un database comune** e, quindi, migliorare le proprie prestazioni nella lotta alla criminalità e al terrorismo. Anche se per ora non c'è alcuna certezza, è plausibile pensare che la proposta giunga dai sottoscrittori del Trattato di Prüm del 2005 (ovvero Austria, Belgio, Francia, Germania, Lussemburgo, Olanda e Spagna e, dal 2009, anche Italia). Nell'accordo, infatti, è già prevista la condivisione del DNA dei condannati per reati sul territorio degli Stati dell'UE e il conseguente impiego dell'intelligenza artificiale, e soprattutto, questi Paesi hanno sempre sollecitato una maggiore integrazione nel settore.

La proposta potrebbe essere una diretta reazione ai più recenti documenti in materia dell'uso dei dati biometrici promossi dall'Unione Europea. Nel luglio dello scorso anno, infatti, la Commissione ha rilasciato delle linee guida sull'uso dell'intelligenza artificiale nel trattamento di queste informazioni con specifico riferimento al sistema del riconoscimento facciale automatico. Nel concreto, il testo indica una sospensione di 5 anni dell'uso dell'identificazione tramite le caratteristiche del viso per permettere di studiare più approfonditamente il tema della privacy legato all'impiego di queste tecnologie. Da tale studio è emerso un documento ("Study on face identification technology for its implementation in the Schengen information system") che valuta se effettivamente le tecnologie oggi disponibili siano in grado di coniugare sicurezza collettiva e tutela individuale, in un'ottica di applicabilità al Sistema Schengen. Il problema che si pone riguarda soprattutto quando e per chi utilizzare questo tipo di strumento (potenziali criminali, cittadini ordinari, etc…), ma anche in che modo e in quali luoghi (aeroporti, stazioni ferroviarie, etc…). Anche se lo studio non ha un valore vincolante, esso illustra gli indirizzi che potenzialmente

"Il problema che si pone riguarda soprattutto quando e per chi utilizzare questo tipo di strumento"

potrebbe assumere la Commissione europea nello sviluppo di future politiche sul tema.

L'oggetto della contesa, ovvero il riconoscimento facciale, rientra nella categoria del trattamento dei dati biometrici. A questa definizione sono riferibili tutti quegli elementi attraverso i quali è possibile identificare univocamente una persona fisica. Si tratta di caratteristiche universali, esclusive, permanenti e in grado di essere catalogate. Generalmente, queste proprietà possono essere fisiologiche e quasi immutabili (come ad esempio impronte digitali, altezza, colore e dimensione dell'iride, forma delle orecchie, fisionomia facciale, sagoma/palmo della mano, vascolarizzazione dell'occhio) oppure comportamentali (voce, grafometria, andatura e gestualità) e legate allo stato psicofisico del soggetto. Una volta incamerati questi dati è necessario che vengano confrontati: nel caso di un'impronta digitale si dovrà fare in modo che l'immagine o il codice associato memorizzati possano incontrarsi con il dito del soggetto in questione (basti pensare agli scanner che utilizzano il "match on board"). Per questo è necessario che le applicazioni in questione dispongano almeno di due componenti: un hardware in grado di raccogliere le informazioni e un software in grado di fare un match (cioè sovrapporre i due elementi).

"L'uso dei dati biometrici è molto discusso, perché le sue tecnologie trovano numerose applicazioni in ambito militare e civile"

Quello dell'uso dei dati biometrici è un tema molto discusso, soprattutto perché le diverse tecnologie ad esso riferibili trovano numerose applicazioni, sia in ambito militare, sia in ambito civile. Inoltre, **il trattamento di queste informazioni pone anche problemi etici non indifferenti relativi alla privacy ed è questo il motivo che il più delle volte trova i legislatori restii a prevederne un utilizzo incontrollato**. In Europa, il testo normativo più dettagliato e recente al riguardo è il General Data Protection Regularion (GDPR - Regolamento n. 679 del 2016), in vigore dal 25 maggio 2018. La legge va a disciplinare la protezione dei dati a tutti i livelli, ma chiaramente ad essere privilegiato è l'aspetto legato alle comunicazioni digitali, dove è sempre più facile acquisire o rilasciare dati sensibili, anche inconsapevolmente.

L'obiettivo del Regolamento n. 679 è garantire la massima protezione dei dati sensibili per i cittadini dell'Unione europea, con particolare il riferimento alle caratteristiche biometriche. Secondo l'articolo 9, il trattamento degli elementi in grado di individuare univocamente un soggetto è vietato, fatto salvo alcune eccezioni espressamente previste dalla normativa. Si tratta innanzitutto del caso in cui l'interessato presti il suo consenso al trattamento dei dati. Ci sono poi situazioni ammesse per quanto riguarda la sicurezza collettiva per esempio nei luoghi di lavoro e nella tutela dell'interesse pubblico, oppure se si tratta di interessi vitali e il soggetto non è in grado di fornire il proprio consenso. Negli articoli successivi, infine, il Regolamento prevede l'obbligo per gli Stati membri di predisporre un registro per il trattamento dei dati. Il GDPR ha portata generale e di conseguenza si applica anche alle attività delle Forze dell'Ordine e ai relativi strumenti di intelligenza artificiale che possono essere adottati dai singoli Stati per implementare l'azione degli agenti.

"EURODAC e ECRIS"

Attualmente a livello europeo esistono due sistemi di coordinamento per la raccolta e l'utilizzo di dati biometrici. Il primo è **Eurodac** (European dactyloscopie), il sistema di dattiloscopia integrato istituito nel 2000 per tenere traccia delle impronte digitali dei richiedenti asilo e dei migranti irregolari presenti sul territorio dell'UE. Il secondo, invece, è **Ecris** (European criminal records information system), il database sui casellari giudiziari attivo dal 2012 per la condivisione delle informazioni tra i tribunali. Questo sistema, basandosi sul mutuo riconoscimento delle decisioni giudiziarie, prevede anche lo scambio di informazioni riguardo i condannati (tra cui le impronte digitali). Per quel che concerne gli sviluppi più recenti, nel documento programmatico 2019-2021 dell'Europol è prevista l'implementazione del comparto ICT (Information and communication technologies) attraverso anche l'utilizzo di dati biometrici. In particolare, nella voce dedicata al Sistema informativo dell'Europol (Eis), si fa riferimento all'intelligenza artificiale per quanto riguarda il Sistema automatico di identificazione biometrica (Abis, Automated biometrics idedintification system), il Sistema di riconoscimento facciale

(Frs, Face recognition system) e il sistema Eres (Enhanced risk entities solution). Tali strumenti vanno ad integrare quelli del Sistema informativo di Schengen (Sis II), del Sistema di informazione per i visti (Vis), della Rete per la registrazione dei nomi dei passeggeri (Pnr), nonché dello stesso Eurodac e del Trattato di Prüm. In sintesi, l'obiettivo è di avere una raccolta dati sempre più corposa e utile a garantire sicurezza sul territorio europeo.

"La situazione in Italia"

In Italia dal 1996 ad oggi si sono succedute una serie di disposizioni volte a tutelare la privacy dei cittadini, giungendo alla sintetizzazione nel Testo Unico del 2003 (Codice della privacy) delle diverse norme prodotte. In riferimento ai dati biometrici, è possibile evidenziare l'adozione del "Sistema automatizzato di identificazione delle impronte" (Afis) da parte della Polizia di Stato. Successivamente, con l'entrata in vigore del GDPR il Codice della privacy è stato aggiornato con il decreto legislativo 101 del 2018.

In attesa degli sviluppi del dibattito in seno alla Commissione europea e tra gli Stati membri, è da notare come negli ultimi anni ci siano già stati dei passi avanti per quanto riguarda sistemi di rilevazione video (che quindi presentano del potenziale in merito al rilevamento facciale). Un esempio di tale avanzamento possono essere le telecamere utilizzate in alcuni stadi, in grado di utilizzare lo zoom per ingrandire dei dettagli senza però perdere la ripresa del contesto. In Italia, per esempio, vengono utilizzati dai Gruppi operativi di sicurezza (Gos) della Polizia di Stato per monitorare le attività delle tifoserie al fine di garantire sicurezza sugli spalti. Tale tecnologia è in grado di rilevare in alta definizione il viso degli spettatori seduti sulle tribune, ma le telecamere non dispongono di quei software necessari per sovrapporre le immagini rilevate con quelle di un possibile archivio dati. Per ora quindi è indispensabile la presenza di un operatore che svolga questa attività, dato anche il contesto di applicazione. Diverso è il caso, invece, del software Sari, utilizzato dalla Polizia di Stato per l'identificazione facciale attraverso la rete di videocamere di sorveglianza urbane. Grazie a questo strumento, le autorità sono in grado di avere riscontri sia dalle immagini (con il sistema

Enterprise), sia dai video (con il sistema Realtime). Il software in questione opera grazie ad un algoritmo, che utilizza informazioni di un apposito schedario predisposto dalla Polizia di Stato.

Viste alcune delle tecnologie già in uso e le direttive UE in materia, appare evidente che il dibattito sull'uso dei dati biometrici a scopi securitari sia ancora intricato. Sebbene il GDPR del 2016 ponga diversi paletti, esso non esclude affatto la possibilità da parte degli Stati di adottare strumenti che prevedano l'utilizzo di queste informazioni. Di fatto, sotto il cappello di situazioni "di interesse pubblico" potrebbero ricadere innumerevoli contesti. Per le Forze di Polizia l'uso di algoritmi in grado di associare in pochi secondi l'immagine di un volto ad un nome, come anche un timbro vocale ben definito ad un soggetto, significa velocizzare le procedure, ma anche prevenire e monitorare al meglio alcune situazioni potenzialmente rischiose. Ciò sempre nel rispetto delle tutele previste per gli eventuali indiziati.

Inoltre, allo stato dell'arte, **ci sono dei criteri tecnici da considerare per quanto riguarda l'affidabilità dei dati biometrici stessi**. Ad esempio, sebbene il riconoscimento facciale presenti una grande praticità per alcuni suoi aspetti (in particolare l'universalità dell'informazione e la catturabilità della stessa), al contempo risultano bassi i valori di unicità e immutabilità nel tempo. Tuttavia, unendo più sistemi (ad esempio riconoscimento facciale e dell'iride) si può garantire la totale corrispondenza con il soggetto. Perciò. la proposta avanzata dalle Forze dell'Ordine dei 10 Paesi europei di condividere le informazioni sul riconoscimento facciale potrebbe risultare molto utile nel contrasto alle attività criminali e ai fenomeni terroristici e rappresenterebbe un importante passo avanti nell'integrazione dei sistemi di sicurezza. Le opportunità nonché i relativi rischi di condividere informazioni del genere, quindi, rappresentano una sfida importante sia per la sicurezza collettiva che per i legislatori. Trattasi quindi di una sfida che potrà essere vinta tenendo conto di entrambi i lati della medaglia e bilanciando gli interessi di autorità e cittadini.