

Quando un video o un'immagine con identificazione di una o più persone riprese viene proposto all'attenzione collettiva è del tutto legittimo chiedersi e chiedere da dove sia stato recuperato. In particolare, quando il video proviene da una manifestazione di piazza e sembra essere stato realizzato dal punto di vista delle forze dell'ordine è non solo legittimo ma anche doveroso stabilire da chi sia stato realizzato, con quali finalità e se la conservazione e il trattamento siano conformi alla legge. Non si tratta di una questione secondaria rispetto al contenuto del filmato, poiché non solo la diffusione di un video (o di un'immagine) acquisito dalle forze di polizia, ma la stessa acquisizione e conservazione rappresentano la luna e non il dito, essendo vietata la schedatura.

Il d.lgs. 51/2018¹, che recepisce una direttiva europea, nel ribadire che le forze dell'ordine possono realizzare filmati solo per finalità istituzionali (per esempio conservare traccia degli interrogatori, acquisire le prove di un delitto ecc.), disciplina le modalità e i tempi di conservazione e cancellazione, i soggetti autorizzati ad accedere agli archivi, i titolari del trattamento e le sanzioni per le violazioni). Ne consegue che le forze di polizia non sono autorizzate a filmare una persona non sospettata di aver commesso un reato o che non sia la potenziale vittima di un reato. E che, se autorizzate per finalità istituzionali, non possono diffondere le immagini acquisite. Nel 2020 il Garante della privacy² ha sanzionato il Ministero dell'Interno in quanto titolare del trattamento per non aver adottato tutte le misure necessarie a impedire la diffusione su internet di un filmato realizzato da un operatore di polizia con il proprio smartphone all'interno di un commissariato per finalità istituzionali (la persona ripresa era stata fermata e aveva reagito con violenza all'arresto e il filmato, realizzato su incarico di un dirigente, aveva l'obiettivo di documentare la necessità dell'uso della forza).

A proposito dell'impiego in spazi aperti al pubblico di sistemi di categorizzazione biometrica, la Risoluzione del Parlamento Europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale³, che ha portato all'attuale formulazione dell'Artificial Intelligence Act⁴, approvato a giugno di quest'anno, afferma "il diritto degli individui non solo a essere identificati correttamente ma anche a non essere identificati, "salvo quando richiesto per legge per interessi pubblici imperativi e legittimi" e avverte che questi sistemi potrebbero essere utilizzati dalle autorità di polizia per classificare le persone in base alla loro etnia o al loro orientamento politico e ne chiede quindi il bando sia ex post sia in tempo reale, almeno fino a quando "le norme tecniche non possano essere considerate pienamente conformi con i diritti fondamentali, i risultati ottenuti siano privi di distorsioni e non discriminatori, il quadro giuridico fornisca salvaguardie rigorose contro l'utilizzo improprio, un attento controllo democratico e adeguata vigilanza, e vi sia la prova empirica della necessità e proporzionalità della diffusione di tali tecnologie".

Per quanto la pratica della "schedatura" anche attraverso le foto e i video sia vietata, tutta coloro che fanno o hanno fatto politica in qualche forma pubblica o che abbiano partecipato

a una manifestazione devono immaginare di essere presente in qualche database. A questo relativamente ridotto gruppo si aggiungono tutte quelle persone che, per le più varie motivazioni, sono (o potrebbero essere) oggetto di attenzione nell'ottica di prevenzione e di repressione dei reati, senza contare tutte quelle che hanno precedenti penali o di polizia⁵. Del resto collaboriamo attivamente e perfino gioiosamente a questa schedatura di massa, fotografando e filmando in ogni occasione e condividendo su chat e social. Appartiene al passato remoto, ormai, l'atteggiamento di sospetto verso chi usava una macchina fotografica durante una manifestazione di piazza: si temeva proprio la schedatura che però, all'epoca, richiedeva un lavoro lungo e faticoso per la catalogazione delle immagini analogiche. Per questo motivo la schedatura era, almeno in parte, più mirata, perché è sostanzialmente inutile accumulare informazioni che non si è in grado di utilizzare. Ciò nonostante le informazioni (non solo le immagini), una volta acquisite spesso non venivano distrutte, nemmeno a seguito di un cambiamento di ordinamento statale. Il versamento negli Archivi di Stato dei casellari politici delle Questure, per esempio, ha permesso di verificare che i fascicoli dei "sovversivi", in parte costituiti durante il fascismo e in parte anche precedenti, erano stati "ereditati" dalla polizia della Repubblica antifascista⁶. E quello italiano non è ovviamente un caso isolato: Herta Müller, premio Nobel per la letteratura nel 2009, per esempio, ha raccontato di aver visto negli archivi della polizia della Romania democratica il fascicolo che la Securitate di Ceaușescu le aveva intestato.

La schedatura attraverso le immagini è resa quasi automatica dalla tecnologia disponibile, quindi in molti casi non è motivata né da obiettivi di garanzia dell'ordine pubblico né da intenti persecutori: semplicemente la tecnologia c'è ed è disponibile sostanzialmente per chiunque, quindi viene utilizzata. Se Google (tra gli altri servizi di cloud storage) offre, tra gli altri strumenti di aggregazione delle proprie foto in base a diversi criteri (a partire dalla geolocalizzazione), il riconoscimento facciale agli utenti dell'app di archiviazione delle immagini, perfino se una persona è stata ripresa di spalle, è ingenuo ritenere che le forze di polizia utilizzino strumenti meno sofisticati di quelli che abbiamo a disposizione quasi tutte, anche se non necessariamente in maniera legittima.

La tecnologia (a partire dalla presenza dei metadati in ogni file, che sono anche utili a stabilire quale device abbia scattato una foto o realizzato un filmato digitale) risolve la maggior parte dei problemi connessi all'archiviazione e rende possibile l'estrazione puntuale da immense banche dati delle immagini e delle informazioni che servono, quando servono. Il punto è proprio questo: a cosa servono e come si possono usare?

Il Parlamento Europeo, nella Risoluzione già citata, individua diversi punti sostanziali di cautela e pone molti "paletti" all'impiego dell'IA da parte delle forze dell'ordine e della magistratura, mettendo in guardia dai molti rischi connessi alla sorveglianza di massa e all'utilizzo dei sistemi di previsione, sia in materia di prevenzione dei reati sia di giustizia predittiva, a fronte della "promessa [...] non sempre mantenuta", che "l'uso sempre più frequente dell'IA nel diritto penale [...] ridurrà determinati tipi di reati e favorirà l'adozione

di decisioni più obiettive” e precisando che, comunque, molti strumenti di IA⁷ sono “illegali ai sensi dell’acquis dell’Unione in materia di protezione dei dati e della relativa giurisprudenza”.

Rileva, infatti, che “l’utilizzo dell’IA nelle attività di contrasto comporta una serie di rischi potenzialmente elevati, e in alcuni casi inaccettabili, per la protezione dei diritti fondamentali degli individui, quali processi decisionali opachi, vari tipi di discriminazione [...], nonché rischi per la protezione della vita privata e dei dati personali, per la protezione della libertà di espressione e informazione, la presunzione di innocenza, il diritto a un ricorso efficace e a un processo equo nonché rischi per la libertà e la sicurezza degli individui”.

Rammenta, inoltre, che “il moderno diritto penale si basa sull’idea che le autorità reagiscono a un reato dopo che è stato commesso, senza supporre che le persone siano pericolose e debbano essere sorvegliate costantemente per prevenire possibili illeciti”. Appoggia, inoltre, le raccomandazioni del gruppo di esperti sull’IA della Commissione a favore del divieto del sistema di *scoring* su larga scala dei cittadini poiché “indebolisce il principio di non discriminazione e non può essere considerato conforme ai diritti fondamentali, in particolare la dignità umana, come sancita dal diritto dell’Unione”.

Gli archivi italiani

Dal 2018 il Ministero dell’Interno dispone del Sistema automatico di riconoscimento immagini (SARI), che funziona come nei film: effettua “una ricerca computerizzata nella banca dati SSA-AFIS⁸ e, grazie a due algoritmi di riconoscimento facciale, è in grado di fornire un elenco di immagini ordinato secondo un grado di similarità”⁹. Il Ministero non precisa che il sistema, oltre a questa funzione, definita Enterprise, implementa anche una funzione di riconoscimento Real time, che confronta i volti dei soggetti ripresi dalle telecamere installate in un determinato luogo e li confronta con una *watch-list* la cui grandezza è dell’ordine delle decine di migliaia di soggetti, a supporto di operazioni di controllo del territorio in occasione di eventi e/o manifestazioni, con la generazione di alert quando nel video appaiono individui presenti nella *watch-list*. La funzione Real time è stata messa momentaneamente in stand by fino alla fine di quest’anno e il Garante della privacy la ritiene in contrasto con le norme nazionali ed europee, poiché è sprovvista di un quadro normativo di riferimento e “realizzerebbe un trattamento automatizzato su larga scala che può riguardare anche persone presenti a manifestazioni politiche e sociali, che non sono oggetto di ‘attenzione’ da parte delle forze di Polizia”¹⁰.

Stando a quanto afferma Reco 3.26, l’azienda scelta dal Ministero dell’Interno per il SARI, la ricerca tra 20 milioni di volti richiede un secondo¹¹ e il Ministero, in risposta all’interrogazione parlamentare dell’on. Sensi del 5/2/2020, ha comunicato che “nella banca dati SAS-AFIS sono presenti, attualmente, 17.592.769 cartellini fotosegnalatici, acquisiti a norma di legge, corrispondenti a 9.882.490 individui diversi, di cui 2.090.064 si riferiscono a

cittadini italiani”¹². Il che vuol dire che il database utilizzato dal SARI è composto in maggioranza da fotosegnalazioni di persone straniere presenti in Italia o transitate dall'Italia.

Da dove arrivano queste immagini e sulla base di quali norme di legge sono state acquisite?

Nell'AFIS sono ovviamente conservati i dati biometrici delle persone condannate in sede penale, ma anche – non altrettanto ovviamente – quelli degli immigrati e delle persone che hanno chiesto la protezione internazionale. Non è possibile sapere a quali nazionalità appartengano gli oltre 7 milioni di cittadini stranieri inseriti nel *database* AFIS né avere statistiche sull'utilizzo del sistema SARI: le Questure cui i ricercatori dell'Hermes center for transparency and digital human rights – organizzazione impegnata a promuovere e sviluppare la consapevolezza e l'attenzione sul tema dei diritti digitali – hanno posto i quesiti tramite accesso civico hanno negato l'accesso a queste informazioni. Né si conoscono le motivazioni che giustificano l'inserimento. L'elevato numero di persone straniere presenti nel database fa sospettare che esso sia almeno parzialmente alimentato attraverso il collegamento con l'EURODAC (European Asylum Dactyloscopy), contenente le impronte digitali dei richiedenti asilo e degli stranieri irregolari che vengono segnalati sul territorio europeo o dall'inserimento, nel database, dei dati del Sistema di gestione dell'accoglienza (SGA), utilizzato al fine di identificare i migranti¹³, poiché chi richiede il permesso di soggiorno o ne richiede il rinnovo è sottoposto a fotosegnalamento¹⁴.

Aver acquisito i dati biometrici in maniera legale non giustifica però che questi stessi dati vengano utilizzati in un database che ha l'obiettivo di identificare gli autori di reati, soprattutto perché gli algoritmi di riconoscimento facciale hanno dimostrato la loro fallibilità quando ricercano un match con foto di persone diverse (per genere e colore della pelle) da quelle utilizzate per la fase di learning (uomini caucasici). *Wired*, riportando i risultati di una ricerca del MIT, scrive che “con gli uomini di carnagione chiara gli algoritmi sono stati precisi il 99% delle volte, mentre la percentuale scende fino al 35% con donne dalla pelle scura”¹⁵.

Sul tema dell'immigrazione, purtroppo, il legislatore europeo ha scelto di non estendere (come sarebbe stato giusto) alle persone in movimento la protezione garantita ai cittadini europei e non ha adottato un divieto ai sistemi di profilazione di tutte le persone in base alle loro caratteristiche sensibili (sesso, etnia, cittadinanza, religione, orientamento politico ecc.), dando invece priorità all'obiettivo di un'illusoria sicurezza basata sull'esclusione e sul pregiudizio: “migranti e stranieri sono rappresentati come popolazioni da dover controllare, tracciare e sorvegliare in quanto fuori dai confini e dunque dalla legge. Non è previsto, come per tutti gli altri cittadini o legalmente residenti all'interno dell'Unione Europea, che sia determinata una ragione specifica per la quale le persone in movimento debbano essere controllate poiché è la loro intrinseca situazione che le rende oggetto di tale sorveglianza”¹².

Maria Pia Calemme

1. <https://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/sg>. [↔]
2. Provvedimento del 26 novembre
(<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9522206>). Sulla mancata osservanza delle norme si veda anche l'ordinanza ingiunzione del Garante della privacy del 24/2/2022 che ha sanzionato il Ministero dell'Interno per aver condiviso con i media immagini acquisite per finalità istituzionali (<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9766469>). [↔]
3. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_IT.html. [↔]
4. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf. [↔]
5. I precedenti di polizia sono tutti quei dati che le forze dell'ordine (comprese le polizie locali e non meglio specificate "altre strutture di vigilanza") raccolgono nel corso della loro attività e registrano presso il centro di elaborazione dati (CED) del Ministero dell'Interno - Dipartimento di pubblica sicurezza, in forza della legge 121/1981 che l'ha istituito. I dati nel CED dovrebbero restarvi per un tempo massimo indicato dalla legge (con il DPR 15/2018 sono stati stabiliti i termini di conservazione per categorie di dati, dai 3 ai 30 anni), ma spesso non vengono aggiornati o cancellati se non si presenta un'apposita istanza al Ministero dell'Interno. Nell'archivio sono presenti, tra gli altri, dati relativi a persone imputate in processi penali che poi sono state assolte o destinatarie di una querela successivamente ritirata. [↔]
6. Si veda, per esempio, <http://www.archiviodistatobologna.it/it/node/1025>, che dà conto della presenza di 8.644 fascicoli personali di "persone pericolose per la sicurezza dello Stato", testimoniando la "schedatura politica dal 1872 al 1983 di anarchici, repubblicani, socialisti, comunisti ma anche persone ritenute a vario titolo potenzialmente pericolose e per questo poste sotto sorveglianza". [↔]
7. Si fa riferimento a: riconoscimento automatizzato delle targhe, identificazione di chi parla, identificazione vocale, tecnologie di lettura labiale, analisi di segnali acustici (algoritmi di rilevamento di colpi di arma da fuoco), ricerca autonoma e analisi di database identificati, previsioni (polizia predittiva e analisi della scena del crimine), strumenti di rilevamento dei comportamenti, strumenti avanzati di autopsia virtuale per contribuire a determinare la causa di morte, strumenti autonomi per identificare le frodi finanziarie e il finanziamento del terrorismo, monitoraggio dei social media (estrazione e raccolta di dati per l'estrazione di connessioni) e sistemi di sorveglianza automatica che integrano diverse capacità di rilevamento (come il rilevamento cardiaco e le videocamere termiche). [↔]
8. Automated Fingerprint Identification System, che contiene le impronte digitali, i dati biometrici e le foto e che quindi sarebbe più corretto definire ABIS (Automated Biometric Identification System) o MBIS (Multimodal Biometric Identification Systems). [↔]
9. <https://www.interno.gov.it/it/notizie/sistema-automatico-riconoscimento-immagini-futuro-diventa-realta>. [↔]
10. <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575842>. [↔]
11. <https://www.reco326.com/it/storie-di-successo/29-sicurezza-pubblica-per-ministero-dell-interno-e-polizia-di-stato>. [↔]
12. <https://protecht.hermescenter.org>. [↔] [↔]
13. <https://www.agendadigitale.eu/sicurezza/privacy/sari-vantaggi-e-rischi-del-riconoscimento-facciale-nella-pubblica-sicurezza/>. [↔]
14. "Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero" (d.lgs. 286/1998). [↔]
15. <https://www.wired.it/attualita/tech/2018/09/27/sari-riconoscimento-facciale/>. [↔]