Anatomia legale del riconoscimento facciale

di *Martina Lo Monaco* e *Jacopo Scipione*

SOMMARIO: 1. Introduzione. – 2. Il quadro legislativo europeo sul riconoscimento facciale. – 3. Due casi studio: Clearview AI e SARI. – 4. Conclusioni.

1. Introduzione

I sistemi di riconoscimento biometrico si stanno facendo strada in modo sempre più prepotente nella nostra vita quotidiana e nella società. Si tratta di tecnologie particolarmente invadenti, poiché implicano la raccolta, la categorizzazione e il riconoscimento di dati inerenti al corpo umano. Il riconoscimento facciale, raccogliendo informazioni sul nostro viso, tratto più peculiare di ogni persona, ne rappresenta l'esempio più emblematico. La sua intrusività, tuttavia, costituisce una minaccia alla vita privata e alla dignità delle persone, accompagnandosi al rischio di ripercussioni negative sui diritti umani e sulle libertà fondamentali.

2. Il quadro legislativo europeo sul riconoscimento facciale

Come sta accadendo già per l'Intelligenza Artificiale (IA), i sistemi di riconoscimento facciale sono stati in questi ultimi anni sotto la lente d'ingrandimento delle istituzioni europee, con risultati spesso discordanti.

Lo scorso 21 aprile la Commissione europea ha pubblicato la sua prima Proposta di Regolamentazione sull'IA, altresì chiamato *AI Act* [1]. Optando per un approccio basato sulla c.d. "piramide di rischio", la Proposta classifica le applicazioni di IA in tre diverse categorie: sistemi vietati, sistemi ad alto rischio e sistemi a rischio medio/basso. Prima di entrare nel merito delle disposizioni sull'uso dei sistemi di riconoscimento facciale, la Commissione fornisce una nozione tecnica dei sistemi di identificazione biometrica. In particolar modo, opera una chiara distinzione tra sistemi di identificazione biometrica remota "in tempo reale"

[1] Si veda Commissione europea, *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione*, COM/2021/206.

e "a posteriori": i primi implicano l'uso istantaneo di materiale rilevato dal vivo; i secondi trattano i dati in differita, cioè in un momento posteriore alla raccolta. Pur implicando entrambi in egual misura il riconoscimento facciale, la Commissione rivolge particolare attenzione al primo dei due. Infatti, solo i sistemi di identificazione biometrica remota "in tempo reale" sono stati classificati come pratiche di IA vietate. L'articolo 5, paragrafo 1, lettera d) ne vieta pertanto l'immissione sul mercato, la messa in servizio e l'uso. Prevede, tuttavia, alcune eccezioni che ne legittimano l'impiego, ove questo sia giustificato dal perseguimento di obiettivi particolarmente rilevanti, come, *inter alia*, la ricerca di vittime di reato o di minori scomparsi. I sistemi di identificazione biometrica "a posteriori", invece, sono inseriti nella più permissiva categoria delle IA "ad alto rischio". I sistemi ad alto rischio possono essere utilizzati, a condizione che siano rispettati una serie di requisiti, come la predisposizione di un sistema di gestione dei rischi, una serie di obblighi informativi per gli utenti, e segnatamente il rispetto dell'articolo 14, relativo alla sorveglianza umana.

L'assetto normativo così risultante presenta però diverse problematiche. *In primis*, la dottrina non ha mancato di osservare che un divieto, così corredato di ampie eccezioni

[2], non somiglia poi tanto a un divieto. Sono certamente nobili le ragioni che spingono a ricorrere a ogni mezzo per cercare le vittime di reato e i minori scomparsi. Più politiche, quelle legate alla prevenzione di "minacce" e attacchi terroristici. Quasi giustizialiste, quelle legate alla ricerca degli autori o sospettati della lunga lista di reati di cui al sub iii). In secondo luogo, non sussistono restrizioni sulla vendita di tali tecnologie al di fuori dei territori dell'UE. Ciò significa che le imprese dell'UE possono vendere liberamente i loro prodotti a Stati terzi, i quali potrebbero sfruttarli per fini repressivi. In terzo luogo, come già spiegato, i sistemi di identificazione biometrica remota "a posteriori" sono permessi. Orbene, ancorché il fatto che il controllo dei dati biometrici avvenga a posteriori offra maggiori garanzie rispetto alla scansione "in tempo reale", ci si domanda se il differimento temporale sia sufficiente a giustificare una tale disparità di regolamentazione. I sistemi "in tempo reale" sono stati vietati soprattutto sulla scorta del timore che possano essere sfruttati per scansionare i partecipanti

[2] Ivi, art. 5, paragrafo 1, lettera d), sub i), ii) e iii): "*i) la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico; iii) il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio 62 , punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, come stabilito dalla legge di tale Stato membro*".

a manifestazioni per i diritti civili o proteste antigovernative, come pare stia già avvenendo in alcuni Stati dall'indole più autoritaria. Tuttavia, legalizzare i sistemi "a posteriori" rischia di vanificare anche il divieto di quelli "in tempo reale": basterebbe, infatti, registrare i filmati delle manifestazioni e passarli al setaccio successivamente, dopo un lasso di tempo ritenuto congruo perché non si possa parlare di riconoscimento "in tempo reale". Anche i sistemi "a posteriori", dunque, costituiscono una grave minaccia per la riservatezza, e un loro abuso rischia di trasformarli in potentissimi strumenti di caccia all'uomo.

Il Parlamento europeo, al contrario, ha una posizione più netta sul riconoscimento facciale. Nella risoluzione del 6 ottobre 2021 riguardante l'IA e il diritto penale, il Parlamento ha chiesto espressamente di vietare l'uso del riconoscimento facciale negli spazi pubblici e l'uso dei *database* privati, come Clearview AI. Ricordando il parere del Comitato europeo per la protezione dei dati[3], il Parlamento ha espresso grande preoccupazione per l'uso di tali banche dati private da parte delle autorità degli Stati membri, per via della loro non conformità con il regime di protezione dei dati dell'UE[4].

Volgendo lo sguardo alla normativa nazionale, si segnala che l'Italia è, a oggi, il primo paese dell'Unione a vietare il riconoscimento facciale nei luoghi pubblici. La recente approvazione del D.L. Capienze [5] alla fine del 2021, infatti, è andata a sospendere l'installazione e l'utilizzazione di impianti di videosorveglianza operanti attraverso l'uso di dati biometrici, rimandandola almeno fino al 2023, anno in cui, presumibilmente, l'*AI Act* sarà stato approvato nella sua versione definitiva. È comunque prevista un'eccezione al divieto di questa tecnologia, per la prevenzione e repressione dei reati o l'esecuzione delle pene. Ancora una volta, le opinioni contrastanti non mancano [6]. Infatti, come già osservato per l'*AI Act*, anche qui le eccezioni sembrano ampie, talmente ampie da legittimare ogni uso già in atto di tali sistemi. Il divieto così configurato potrebbe limitarsi a essere, in altri termini,

[3] Si veda European Data Protection Board, *EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination*, 21 giugno 2021.

[4] Si veda Parlamento europeo, *Proposta di Risoluzione del Parlamento europeo sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale*, (2020/2016(INI)).

[5] Decreto legge 139/2021, recante «Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali», convertito dalla legge 205/2021.

[6] Si veda A. Longo, *Italia primo Paese a vietare il riconoscimento facciale (con eccezioni)*, Il Sole 24 Ore, 2 dicembre 2021, disponibile su: https://www.ilsole24ore.com/art/italia-primo-paese-vietare-riconoscimento-facciale-con-eccezioni-AEFLRY0?utm_source

una sorta di dichiarazione d'intenti, un gesto simbolico destinato a non cambiare nulla nella pratica.

3. Due casi studio: Clearview AI e SARI

Il tema del riconoscimento facciale è stato portato alla ribalta da cronaca e giuristi come conseguenza della preoccupazione generale che l'uso di tali sistemi già suscita in molti paesi del mondo, con esiti tutt'altro che rassicuranti. Negli Stati Uniti, ad esempio, da anni le forze dell'ordine adoperano software di riconoscimento facciale per affiancare gli investigatori nell'identificazione di sospetti le cui foto siano state catturate in flagranza di reato, generalmente mediante telecamere di sicurezza.

La prima generazione di software utilizzati dalle forze dell'ordine si avvaleva di foto acquisite delle patenti o dalle foto segnaletiche. Tale raccolta di immagini veniva poi processata da algoritmi che attuavano il c.d. "*hashing*". L'*hashing* consiste nel misurare alcuni elementi chiave nella biometrica del viso, quali ad esempio la distanza tra le pupille, tra gli occhi e il naso, la lunghezza relativa della testa, etc. A partire da questi dati, l'algoritmo traccia una geografia univoca del volto, che utilizza poi per trovare corrispondenze (c.d. "*match*") tra le immagini di database e quelle di volta in volta sottoposte ad analisi.

Questi primi software sono stati sbaragliati dall'arrivo di un *player* destinato a diventare il principale attore nel campo: Clearview AI. Fondata nel 2017 dall'eclettico Hoan Ton-That e dal politico repubblicano Richard Schwartz, oggi conta oltre 2.200 clienti tra agenzie governative, compagnie private e persone fisiche. Tra i soggetti che hanno destato maggior scalpore si annoverano le forze di polizia – anche di frontiera – degli Stati Uniti, diverse rinomate università, e persino l'F.B.I.[7].

La caratteristica principale che distacca Clearview AI dai suoi predecessori risiede nel fatto che quest'ultima trae linfa per il proprio *database* attingendo da tutte le fonti *open-source* disponibili online. I *social network* come Facebook e Twitter costituiscono per Clearview AI un'immensa fonte di immagini, caricate spontaneamente dagli utenti e spesso già corredate

[7] A seguito di una fuga di notizie, il sito di notizie Buzzfeednews ha pubblicato, nel febbraio 2020, una lista dei clienti di Clearview AI. Molti soggetti hanno successivamente negato ogni connessione con la società. V. R. Mac - C. Haskins - L. McDonald, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, 2020, disponibile su: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

da tag, cioè da etichette con i nomi delle persone rappresentate. Si stima che l'intero database di Clearview AI comprenda oggi oltre 10 miliardi di *data-point*. In recenti comunicazioni agli investitori la società ha dichiarato di essere proiettata verso il traguardo di 100 miliardi di foto entro la fine dell'anno, il che le permetterebbe di identificare quasi ogni persona sul pianeta[8].

Il processo di "*scraping*", ossia di rastrellamento di dati *open-source* su internet, non è astrattamente vietato. Non c'è dubbio che la raccolta di dati mediante questo processo è stata, fin dall'avvento di internet, indispensabile al suo stesso sviluppo, e lo è ancora per tutte le ricerche e tecnologie che fanno uso di *Big Data*. È tuttavia lecito dubitare che questa prassi, applicata allo sviluppo di tecnologie di riconoscimento facciale e senza un esplicito consenso dei titolari delle immagini, debba essere consentita. Infatti, occorre tenere presente che le fotografie vengono spesso caricate su internet da terze parti, senza che i soggetti rappresentati abbiano prestato il loro consenso o siano anche solo a conoscenza della divulgazione della loro immagine. Ciò costituisce un limite difficilmente superabile per il deficit di consenso, sempre ammettendo che questo venga mai considerato, dagli operatori in questione, come una faccenda degna di riguardo. A ciò si aggiunga che le attività di *web scraping* sono quasi sempre vietate dai gestori di servizi di *social networking*, attraverso esplicite clausole contenute nei termini di servizio.

In tempi recentissimi il Garante italiano si è espresso con riguardo a Clearview AI[9]. Alla società americana è stato ingiunto di eliminare e cessare la raccolta di dati relativi alle persone che si trovano in Italia. L'intervento si colloca sotto l'ombrello del potente strumento del GDPR, il quale, pur essendo un regolamento dell'Unione europea, si applica a tutti i trattamenti di dati che coinvolgono cittadini europei, quale che sia la nazionalità del soggetto che li effettua – il cd. titolare del trattamento. Su queste basi, il Garante accerta una serie di violazioni del GDPR e commina alla società una sanzione amministrativa di 20 milioni di euro. Esso evidenzia che «*la pubblica disponibilità di dati in Internet non implica, per il solo fatto del loro pubblico stato, la legittimità della loro raccolta da parte di soggetti terzi*», e che, pertanto, neanche in questi casi si può prescindere da una legittima base giuridica di trattamento. Volendo calare il principio su un terreno più concreto, tale statuizione del Garante mette in chiaro che il

[8] Si veda D. Harwell, *Facial recognition firm Clearview AI tells investors it's seeking massive expansion beyond law enforcement* – The Washington Post, 16 febbraio 2022, disponibile su: https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/

[9] Garante della Privacy, *Ordinanza di ingiunzione nei confronti di Clearview AI - 10 febbraio 2022 [9751372]*.

semplice fatto di caricare una propria foto su un *social network* non può costituire una sorta di peccato originale a seguito del quale tale foto può essere utilizzata senza remore, e per gli scopi più disparati, da terzi operanti sotto il vessillo del "sono pubblicamente disponibili". Il consenso prestato, ai sensi del GDPR, per il trattamento su quel *social network* rimane vincolato ad esso, e non lo si può far trasmigrare a proprio piacimento su altre piattaforme, né lo si può astrarre fino a considerarlo un consenso *tout court* all'uso della propria foto da parte di chiunque lo desideri.

Anche l'Italia ha un proprio sistema di riconoscimento facciale: SARI. Sviluppato da un'azienda leccese e in uso alla polizia scientifica dal 2017, SARI consta di due sistemi: Enterprise, che opera un riconoscimento "a posteriori", e Real Time, che opera in tempo reale. Stando al capitolato della fornitura, il *database* comprenderebbe circa 10 milioni di immagini, tratte esclusivamente dalla banca dati di foto segnaletiche Afis [10]. Secondo dichiarazioni successive, i *data-point* sarebbero invece 16 milioni. Non è mancato chi, anche in seno al Parlamento, ha sollevato perplessità su questi numeri (che sembrano sproporzionati rispetto all'attività di foto-segnaletica svolta in Italia) e dunque sulla provenienza delle immagini[11].

Il 25 marzo 2021, il Garante per la protezione dei dati personali si è espresso sull'utilizzo di SARI Real Time, esprimendo parere negativo [12]. La scansione indiscriminata e *live* di tutti i volti in un dato luogo, secondo il Garante, opererebbe una forma di videosorveglianza non conforme alle leggi sulla *privacy*. Esso impatterebbe anche sulla riservatezza di persone che non sono oggetto di attenzione da parte della polizia e, in definitiva, rischia di raccogliere una mole di dati smisurata, in totale assenza di consenso e di qualsivoglia base giuridica. Per contro, la versione Enterprise non costituirebbe un nuovo trattamento dei dati, ma solo una nuova modalità, automatizzata, di trattamenti che venivano già effettuati in precedenza, con le basi giuridiche opportune, da agenti umani (raffronto delle foto dei sospettati). L'intervento del Garante, dunque, si allinea con la scelta dell'*AI Act* di trattare con maggiore permissività i sistemi di verifica in differita rispetto ai sistemi in tempo reale.

---

[10] *Capitolato tecnico della procedura volta alla fornitura della soluzione integrata per il Sistema Automatico di Riconoscimento Immagini S.A.R.I.,* disponibile su: https://www.poliziadistato.it/statics/06/20160627-ct-sari--4-.pdf

[11] L'interrogazione parlamentare a risposta scritta dell'on. Federico D'Incà, del 19 settembre 2018 (disponibile su: http://aic.camera.it/aic/scheda.html?numero=4/01149&ramo=CAMERA&leg=18) non ha ancora ricevuto una risposta da parte del Ministero dell'Interno.

[12] Garante della Privacy, *Parere sul sistema Sari Real Time - 25 marzo 2021 [9575877].*

Infine, un problema ineludibile nel dibattito del riconoscimento facciale è che tali sistemi si sono dimostrati spesso fallaci. I c.d. *bias*, sempre presenti nel dibattito sull'IA, interessano soprattutto le persone appartenenti a minoranze etniche, specie gli afroamericani, ma anche le donne e il gruppo demografico di età compresa tra i 18 e i 30 anni [13]. Tali soggetti sono riconosciuti in modo sensibilmente meno accurato rispetto agli uomini caucasici. Ciò potrebbe dipendere da come è stato addestrato il sistema di IA – ossia con campioni di immagini non rappresentativi –, ma anche dal fatto che una cattiva illuminazione può rendere i volti dalla pelle scura più difficili da analizzare.

Ombre, pose e angoli di ripresa anomali costituiscono da sempre una sfida per il riconoscimento facciale. Le tecnologie più recenti tengono in considerazione molte variabili di prospettiva e illuminazione, e finanche la presenza di occhiali e mascherine. Ciò nondimeno si riporta la prassi, negli uffici di polizia, di "photoshoppare" le immagini per renderle più fruibili per il software, con manipolazioni che vanno dalla correzione dei colori, fino a operare ritagli e collage di parti del viso nella speranza di ottenere un *match* difficile[14].

L'intero processo di identificazione non è vincolato da alcuna linea guida o regola ufficiale, ed è condotto a porte chiuse in modo del tutto incontrollato. Non esistono norme che precisano il tipo di manipolazioni delle immagini consentite, o che istituiscono obblighi di controllo e riscontro. Clearview AI dichiara che il proprio *software* costituisce meramente un primo *step* nel processo investigativo, e che tutte le corrispondenze devono essere confermate dall'operatore umano e corroborate da ulteriori indizi. Pur tuttavia, i casi di errore marchiano riportati dalla cronaca [15] dimostrano che gli ulteriori passaggi di conferma del *match* non sempre vengono messi in atto. Né, d'altra parte, sussiste alcuna norma che li imponga, o che istituisca un obbligo, in alcuna fase del processo, di informare l'imputato che il suo riconoscimento è stato operato da un'IA.

---

[13] Si veda P. Grother - M. Ngan - K. Hanaoka, *Face Recognition Vendor Test (FRVT)*, 2019.

[14] Ad esempio, incollando ritagli di occhi aperti su foto che ritraggono il sospettato con gli occhi chiusi. Si veda R. Brandon, *The NYPD uses altered images in its facial recognition system, new documents show*, The Verge, 16 maggio 2019, disponibile su: https://www.theverge.com/2019/5/16/18627548/nypd-facial-recognition-altered-faces-privacy

[15] Per uno dei casi più discussi, si veda A. Robertson, *Detroit man sues police for wrongfully arresting him based on facial recognition*, The Verge, 13 aprile 2021, disponibile su: https://www.theverge.com/2021/4/13/22382398/robert-williams-detroit-police-department-aclu-lawsuit-facial-recognition-wrongful-arrest

Inoltre, uomini e IA tendono a trasmettersi reciprocamente i *bias* di cui soffrono, in un deprecabile circolo vizioso. L'operatore umano deputato a confermare un *match* rischia di soffrire di un *bias* di oggettività: quanto più la macchina gli abbia dimostrato in passato di essere affidabile, tanto meno il controllo sul suo operato sarà obiettivo. In altri termini, una volta che la routine di affidarsi all'IA ha preso piede, il rischio è che l'uomo si limiti a prendere atto del risultato con cieca confidenza, e che il suo controllo sia una vuota formalità. Si perderà così, in nome dell'automazione, della rapidità e dell'efficienza sui grandi numeri, quella scintilla umana che ancora oggi sarebbe indispensabile per razionalizzare tutto il processo, e per evitare quegli errori grossolani in cui talvolta gli algoritmi più sofisticati, ma non l'intelletto umano, incorre.

4. Conclusioni

Vietare radicalmente queste tecnologie appare, ormai, irrealistico. Alla luce della loro diffusione, un divieto assoluto sembrerebbe – per usare un'immagine evocativa – un vano tentativo di chiudere la stalla dopo che i buoi sono scappati. Inoltre, ci priverebbe della possibilità di svilupparne il potenziale virtuoso – e a dispetto del fatto che in questa sede ci si è concentrati più sui rischi, non si può negare che i vantaggi esistono. Ciò che si auspica è, piuttosto, di avere a stretto giro una regolamentazione chiara, tanto per i fornitori quanto per gli utenti.

Per quanto riguarda i fornitori, dovrebbero essere imposte delle linee guida nella progettazione degli algoritmi. In primo luogo, un *database* curato, con campioni rappresentativi di diverse età, genere e nazionalità, con l'inclusione di minoranze etniche. Solo da queste basi si possono muovere i passi per un'IA meno discriminatoria. In secondo luogo, i criteri di identificazione dovrebbero essere trasparenti e ricostruibili, mettendo in evidenza i dati (*data-point* utilizzati), il processo (eventuale alterazione delle immagini) e gli esiti (percentuale di certezza del *match*). In terzo luogo, l'apertura a studi condotti da soggetti indipendenti che possano mettere in luce efficacia e difetti del prodotto.

Per quanto concerne l'uso da parte degli utenti, sembra inaccettabile che, a oggi, le norme di procedura penale dei paesi in cui tali sistemi sono in uso continuino a ignorare sfrontatamente la realtà, ossia che le IA stanno affiancando, quando non soppiantando, i tradizionali metodi dell'identikit e della ricognizione personale (che invece erano debitamente

disciplinati). E ancora, mentre in caso di errore le società produttrici e gli utilizzatori si trastullerebbero nel loro inevitabile gioco del rimbalzarsi le responsabilità, la legge dovrebbe stabilire in modo chiaro dove questa debba risiedere. Spetta, insomma, al legislatore progettare una cornice di controlli e riscontri che possa in qualche modo fornire le necessarie rassicurazioni alla collettività.