FACE TO FACE: IL COMPLESSO RAPPORTO TRA *AUTOMATED FACIAL RECOGNITION TECHNOLOGY* E PROCESSO PENALE[1]

di Ernestina Sacchetto
(Dottoranda di ricerca in Diritti e Istituzioni presso l'Università degli studi di Torino)

SOMMARIO: 1. Un'indispensabile introduzione tecnica; 2. Il volto tra ricognizione e individuazione nell'attuale impianto codicistico; 2.1. Il software S.A.R.I. – sistema automatizzato riconoscimento immagini; 2.2 Il *bias* nei sistemi di *automated facial recognition*; 3. *Facial recognition* e processo penale in Italia; 4. Considerazioni conclusive.

1.- Fra i diversi accertamenti esteriori che è possibile compiere sulla persona[2], negli ultimi anni il volto ha assunto un ruolo di estremo rilievo[3]. I sistemi di identificazione facciale, rispetto ad altri metodi di riconoscimento biometrici[4], presentano il

[1] Testo, rivisto e aggiornato, della relazione tenuta al Convegno ICON·S *Italian Chapter - "Le nuove tecnologie e il futuro del diritto pubblico"*, svoltosi presso l'Università degli Studi di Firenze (Polo delle Scienze sociali di Novoli), nelle date del 22 e 23 novembre 2019. E' stato aggiunto un corredo essenziale di indicazioni bibliografiche e giurisprudenziali, indicando soprattutto le fonti cui si è fatto più diretto riferimento nella relazione.

[2] Cfr. G. Iovane, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza*, Roma 2008, 213.

[3] Cfr. T. Alesci, *Il corpo umano fonte di prova*, Milano 2017, 89. Per un approfondimento v. G. Gulotta, E. M. Tuosto, *Il volto nell'investigazione e nel processo. Nuova fisiognomica Forense*, Milano 2017, 114 e segg.; «*Face recognition with its wide range of commercial and law enforcement applications has been one of the most active areas of research in the field of computer vision and pattern recognition*». J. Zheng, V. M. Patel, R. Chellapa, *Recent developments in Video-based Face recognition*, in AA.VV., *Handbook of biometrics for forensic science*, a cura di M. Tistarelli, C. Champod, Cham 2017, 149; N. Balossino, S. Siracusa, *L'identificazione basata sul volto: metodi fisionomici e metrici*, in https://docplayer.it/18656857-L-identificazione-basata-sul-volto-metodi-fisionomici-e-metrici.html; G. Preite, *Il riconoscimento biometrico. Sicurezza versus Privacy*, Trento 2007, 37 e segg.; F. Cascetta, M. De Luccia, *Sistemi di identificazione personale* in *IlMonDig*, n. 1, Marzo 2004, 49. Per un approfondimento si veda S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, Torino 2013, 33.

[4] «(…) due sono i tratti peculiari e distintivi dei dati biometrici. In primo luogo, i dati biometrici non possono essere rilevati sulla base di una semplice raccolta dati, ma sono il frutto di uno specifico processo tecnico volto ad estrapolare il dato biometrico a partire dalle caratteristiche del soggetto. In secondo luogo, i dati biometrici si riferiscono a caratteristiche uniche del soggetto e, pertanto, sono gli unici dati che consentono un'identificazione univoca della persona a cui si riferiscono». Cfr. L. Greco, A. Mantelero, *Industria 4.0, robotica e privacy-by-design*, in *Diritto dell'Informazione e dell'Informatica (Il)*, fasc.6, 1.12.2018, 875.

vantaggio di non essere *invasivi*, poiché non solo richiedono poca o nessuna collaborazione da parte del soggetto passivo, ma il sistema non risulta nemmeno assoggettabile a cambiamenti comportamentali, volontari o meno, da parte dell'individuo sottoposto al riconoscimento[5].

Il procedimento di identificazione trae evidenti vantaggi dall'impiego di dispositivi informatici[6]; questi infatti consentono di estrarre caratteristiche fisionomiche non direttamente visibili e rendono agevoli confronti e valutazioni metriche[7]. Peraltro, sempre più di frequente, fatti di cronaca mostrano come tramite telecamere di videosorveglianza sia possibile risalire più agevolmente all'autore del reato o all'identificazione della vittima, attraverso l'estrapolazione dell'immagine del volto di una persona[8]. Privati cittadini, aziende e amministrazioni pubbliche hanno cominciato a sviluppare la tendenza a disseminare impianti di videosorveglianza per scopi di tutela e

[5] In particolare, «una grandezza, per essere ritenuta "biometrica", deve possedere i seguenti caratteri: "universalità", deve essere posseduta da ogni individuo; "unicità", non possono esservi due individui con gli stessi caratteri; "permanenza", il carattere non deve essere variabile nel tempo; "collezionabilità", il carattere deve potersi misurare quantitativamente ed essere riproducibile su un supporto». Inoltre, nella scelta di un sistema biometrico, possono divenire centrali parametri diversi come «la "performance", indica le risorse richieste, le modalità e l'ambiente che determina una più accurata identificazione» e il "grado di gradimento", coincidente con il grado di accettazione di una certa metodologia biometrica. Cfr. S. Amato, F. Cristofari, S. Raciti, *op. cit*., 126. «*Personal identification systems based on faces have the advantage that facial images can be obtained from a distance without requiring cooperation of the subject, as compared to other biometrics such as fingerprint, iris, etc*.». J. Zheng, V. M. Patel, R. Chellapa, *op. cit*., 149. D'altra parte, sempre da un punto di vista biometrico, il riconoscimento del volto non è caratterizzato da un'elevata permanenza: le molteplici espressioni del volto, l'età, i radicali cambiamenti nel *look* (capelli, barba, baffi ecc.), la presenza di occhiali, sono esempi di caratteri esteriori che possono mutare nel tempo rendendo difficoltoso il riconoscimento facciale. Oltre a ciò, gli interventi di chirurgia plastica contribuiscono a ridurre la possibilità di *matching* del sistema di riconoscimento. Sul punto si veda Richa Singhi, Akshay Agarwal, Maneet Singh, Shruti Nagpal, Mayank Vatsa, *On the Robustness of Face Recognition Algorithms Against Attacks and Bias*, 2/2020, in https://arxiv.org/pdf/2002.02942.pdf.

[6] Le principali tecniche informatiche impiegate nel riconoscimento del volto sono la PCA (*Principal Component Analysis*)[6], la LFA (*Local Feature Analysis*) e le reti neurali. G. Gulotta, E. M. Tuosto, *op. cit.*, 118.

[7] Il confronto fra i volti si basa sulla definizione di parametri che possono essere sia fisionomici sia metrici. I primi – qualitativi - si basano su regole che rendono meno soggettiva l'interpretazione; i secondi invece – quantitativi - generano valori numerici; entrambi vengono studiati dalle scienze antropometriche.

[8] T. Alesci, *op. cit*., 90; Per un approfondimento sulle modalità con cui le immagini vengono cristallizzate a seguito di una videoripresa trovando ingresso nel processo penale, v. S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino 2018, 303. Cfr. https://www.ilgazzettino.it/italia/cronaca_nera/brescia_ladri_arrestati_riconoscimento_facciale_7_settembre_2018-

prevenzione[9]: ne consegue la potenziale «acquisizione di una moltitudine di fotogrammi, con i quali è possibile riconoscere eventuali fatti di reato»[10]. In tali termini, l'atto di identificare un soggetto ignoto consiste nel comparare delle immagini estrapolate dai sistemi di videosorveglianza con quelle acquisite precedentemente e inserite in un archivio: la qualità del fotogramma influirà notevolmente sull'intero procedimento. Se, per esempio, le riprese sono adeguatamente luminose e ricche di dettagli, saranno per lo più sufficienti confronti fisionomici[11].

Come è noto, lo studio delle caratteristiche del volto richiede l'individuazione di particolari siti anatomici, detti *punti di repere*[12], utili sia per la rappresentazione di

---

3959042.html; https://tg24.sky.it/tecnologia/2020/02/21/riconoscimento-facciale-azienda-italiana.html; https://www.lastampa.it/topnews/primo-piano/2018/09/10/news/sedici-milioni-di-volti-gia-nel-database-e-polemica-sul-riconoscimento-facciale-1.34043997. A titolo esemplificativo cfr. Cass., 18.06.2019, n. 40035 in *CEDCass* m. 277603, Cass., 6.02.2019, n. 32813, in *CEDCass* m. 277086, Cass., 25.10.2018, n. 54 in *CEDCass* m. 274381.

[9] «L'obiettivo è quello di consentire il cd "riconoscimento facciale tra la folla". Il sistema del "*Biometric Optical Surveillance System*" (Boss), secondo un recente studio del *New York Times* consentirebbe di scansionare intere folle ed identificare presunti terroristi. Il riconoscimento facciale avviene attraverso macchine dotate di sensori ad infrarossi che fotografano diverse angolature del volto. I dati così raccolti, vengono poi elaborati da un software, al fine di verificare la corrispondenza con il volto di presunti terroristi catalogati nel *database*». T. Alesci, *op. cit*., 89. Cfr. Cass., 13.05.2019, n. 20527 in *CEDCass* m. 275309. Cfr. https://www.biometricupdate.com/201907/banco-bolivariano-selects-facephi-biometric-digital-onboarding-technology; «*The widespread use of CCTV cameras for surveillance and security applications have stirred extensive research interests in video-based face recognition. (…) Automatic face recognition technology is becoming an indispensable tool for modern forensic investigations*». See X. Wei, C. Li, *Face recognition Technologies for Evidential Evaluation of Video Traces*, in AA.VV., *Handbook of biometrics for forensic science*, a cura di M. Tistarelli, C. Champod, Cham 2017, 190. Sul punto si veda S. Zuboff, *The age of surveillance capitalism. The fight for human future at the new frontier of power*, London 2019, 252.

[10] Cfr. T. Alesci, *op. cit*., 89.

[11] Il volto può essere interessato da processi di invecchiamento, diverse espressioni facciali, variazioni di illuminazione e dello sfondo dell'ambiente circostante, da variazioni di posizioni rispetto alla telecamera, dalla presenza di occhiali etc. E, ancora, «(…) *automated face recognition actually subsumes a number of separate problems. In identity verification, the subject looks straight at the camera under controlled lighting conditions, and their face is compared with the one on file. A related but harder problem is found in forensics, where we may be trying to establish whether a suspect's face fits a low-quality recording on a security video. The hardest of all is surveillance, where the goal may be to scan a moving crowd of people at an airport and try to pick out anyone who is on a list of perhaps as few distributed System*[2], 2008, 264. Per un approfondimento sugli errori derivanti da cattiva illuminazione: Y. Adini, Y. Moses, S. Ullman, *Face recognition: The Problem of Compensating for Changes in Illumination Direction*, in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, v. 19 no. 7 (July 1997), 721-732. In generale si veda S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, Torino 2013, 125.

[12] «I principali punti di *repere* sono: il *nasion* (radice del naso); *glabella* (punto situato al di sopra della

strutture morfologiche sia per la valutazione dei diversi aspetti somatici. A seguito dell'evoluzione tecnologica, il sistema biometrico basato sul riconoscimento del viso è divenuto un processo automatico o semi-automatico che compara e pone in luce le differenze della struttura geometrica del volto, tra cui la configurazione dei suoi attributi e le loro relazioni geometriche[13], compiendo un'analisi metrica dell'immagine e del tessuto della pelle[14]. Se il procedimento è attivato per sorvegliare *live* l'accesso a particolari strutture, il riconoscimento dei volti (*face recognition*) richiede che un sistema informatizzato analizzi in pochi attimi i dati a disposizione e ne ricavi una sorta di "cartografia facciale" che viene confrontata con quelle registrate in precedenza negli archivi degli organi di sorveglianza. Il riconoscimento avviene tramite software che si basano (per lo più) su tecniche neurali[15] che simulano il processo di apprendimento umano. Quando invece si debba procedere all'identificazione in un tempo differito, come per esempio accade nel caso in cui si debba comparare l'immagine di un assassino a quella di un insieme di indagati, il metodo adottato richiede una valutazione fisionomica e metrica per giungere a un giudizio di identificazione o esclusione.

2.- Posto che il volto costituisce una caratteristica fondamentale attraverso cui attribuire l'identità di un soggetto, occorre distinguere due istituti tradizionali del processo penale, l'*identikit* e il riconoscimento facciale[16]. Mentre nel primo caso le tecniche più all'avanguardia permettono la ricostruzione dell'immagine tridimensionale del volto, nel secondo esse consentono un confronto automatico tra l'immagine del soggetto estrapolata dalle telecamere di videosorveglianza e le immagini contenute nei

---

radice del naso, dove la cute è in genere priva di peluria); *pronasale* (punto più sporgente della punta del naso); *naso spinale* (punto corrispondente al sottosetto nasale); *alare* (punto più sporgente dell'ala del naso); *prosthion* (punto superiore del solco naso labiale); *gonion* (margine inferiore del ramo della mandibola); *gnathion* (sporgenza inferiore del mento); *trichion* (punto di attacco dei capelli sulla fronte); *vertex* (punto più alto del cranio); *zygion* (punto più sporgente dello zigomo)». N. Balossino, S. Siracusa, *L'identificazione basata sul volto: metodi fisionomici e metrici*, Security Forum, Edizioni ItasForum, Bergamo 2004, 4. Si veda anche G. Gulotta, E. M. Tuosto, *op. cit*., 114. *hundred known suspects*». R. Anderson, *Security Engineering : a guide to building dependable*

[13] Gli occhi, le sopracciglia, le labbra e il mento. Si veda, *ex multis*, S. Signorato, *op. cit.*, 99.

[14] Durante la rilevazione dei dati, un sensore (ad esempio una telecamera) cattura un'immagine o una serie di immagini del volto del soggetto che vengono convertite in formato digitale. Un algoritmo registra le caratteristiche rilevanti e crea un *template* di dimensioni inferiori rispetto al volto originale rendendo possibile la sua memorizzazione, per esempio, su una *smart card* o su un passaporto, utilizzati per i procedimenti di verifica dell'identità. Per un approfondimento sul discrimine fra software valutativi e non valutativi, si veda S. Signorato, *op. cit*., 100.

[15] Per un iniziale studio sulle tecniche neurali v. http://www.treccani.it/enciclopedia/storia-dei-concetti-e-delle-tecniche-nella-ricerca-sulle-reti-neurali_%28Frontiere-della-Vita%29/.

[16] Cfr. T. Alesci, *op. cit*., 90; G. Gulotta, E. M. Tuosto, *op. cit*., 91 e 109 e segg.

database nazionali degli organi di polizia, ovvero utilizzate per la ricognizione[17]. Com'è noto l'elaborazione dell'immagine di un volto[18] però presenta un livello di affidabilità molto basso: gli esperti di neuropsicologia escludono che la mente sia capace di registrare un volto in modo indelebile nella memoria, poiché il processo di memorizzazione è ricostruttivo e soggetto a continui cambiamenti o interferenze[19]. Oltre a ciò, il volto ricostruito a partire dalle informazioni ricevute da persone offese o dai testimoni in stato di vulnerabilità risulta in generale scarsamente aderente a quello originale[20].

Secondo autorevole dottrina, il riconoscimento dei volti tramite ricognizione costituisce un mezzo di prova maggiormente affidabile in quanto l'elaborazione globale del viso è favorita in modo più agevole dalla distinzione degli uni rispetto agli altri[21]. Tutti i soggetti possono essere ricognitori attivi e il testimone avrà l'obbligo di dire la verità, l'imputato godrà della facoltà di non sottoporsi al compimento dell'atto e l'imputato connesso o collegato potrà rimanere in silenzio[22]. Dal punto di vista passivo, invece, è discusso se il giudice possa sottoporre coattivamente l'imputato alla ricognizione ed impedire eventuali gesti finalizzati ad evitare il riconoscimento. Lo svolgimento del mezzo di prova è descritto dal codice in modo minuzioso: l'atto può essere compiuto nel corso del dibattimento o durante l'incidente probatorio e si svolge nel rispetto del contraddittorio tra le parti[23].

Alla tradizionale attività di riconoscimento disciplinata dall'art. 213 Cpp, si affianca la possibilità di utilizzare le immagini estrapolate dai sistemi di videoripresa per sottoporle, come documenti ex art. 234 Cpp, all'attenzione del testimone e soprattutto all'analisi dei periti[24]. Trattasi di un meccanismo complesso che si riduce comunque a valorizzare il ricordo mnemonico di un soggetto chiamato, anche a distanza di tempo, a stabilire se una tale persona è la stessa vista in precedenza e in occasione del fatto di

[17] P. Tonini, *Manuale di procedura penale[13]*, Milano 2012, 483.

[18] Cd. "*sketch*".

[19] G. Gulotta, E. M. Tuosto, *op. cit.,* 110.

[20] Per un approfondimento sul tema, *ex multis*, v. A. M. Giannini, E. Tizzani, A. D'Amore, *L'identikit: come si aiuta un testimone a ricordare* in *RIC*- 4/2012, p. 284

[21] *Ex* articolo 213 Cpp, con la *ricognizione* un soggetto è chiamato a individuare persone, cose, voci, suoni oggetto di percezione sensoriale. Anche tale mezzo di prova comunque presenta delle criticità. Per un approfondimento si veda, *ex multis,* P. Tonini – C. Conti, *Il diritto delle prove penali,* Milano 2014, 322; G. Gulotta, E. M. Tuosto, *op. cit*., 124 e T. Alesci, *op. cit*., 90.

[22] Cfr. T. Alesci, *op. cit*., 90 e 91.

[23] Cfr. P. Tonini, *Manuale di procedura penale*, Milano 2018, 340; v. anche A. M. Capitta, Ricognizioni e individuazioni di persone nel diritto delle prove penali, Milano 2001.

[24] A. Bernasconi, *La ricognizione di persone nel processo penale. Struttura e procedimento probatorio*, Torino 2003, 52. Si veda anche N. Pascucci, *La natura controversa della ricognizione fotografica*, in *RIDPP* fasc.1, 2017, 287.

reato considerato nel procedimento[25]. Peraltro, secondo la dottrina maggioritaria, tale istituto sfugge del tutto alle garanzie predisposte dal legislatore: il teste non solo è sottoposto ad una domanda suggestiva, ma essendo anche collocato in un contesto poco neutrale, subisce le inevitabili pressioni dettate dall'ambito della testimonianza[26].

L'individuazione, *ex* art. 361 Cpp, costituisce invece «un atto tipico del pubblico ministero, delegabile alla polizia giudiziaria e corredato da minori garanzie difensive»[27]. Tenuto conto della possibilità di ripetere l'atto, la disciplina dell'istituto in esame risulta piuttosto scarna. Peraltro, la suddetta attività di indagine è stata interessata da un'estesa corrente interpretativa giurisprudenziale che gli ha attribuito una natura in senso lato "testimoniale"[28]. Ciò ha consentito di recuperare gli esiti dell'individuazione compiuta ex art. 361 Cpp attraverso la testimonianza confermativa. In tale scenario, individuazione e testimonianza risultano due momenti di una medesima operazione probatoria che si snoda fra indagini e dibattimento[29]. L'adozione dell'istituto dell'individuazione desta più profonde incertezze se si considera che si tratta di un atto espressamente attribuito al pubblico ministero ma non vietato alla polizia giudiziaria[30].

Oltre all'individuazione tradizionale, la polizia giudiziaria può altresì compiere un'individuazione fotografica, sia su delega del pubblico ministero sia di propria iniziativa, in forza del combinato disposto degli artt. 55 e 348 Cpp. Secondo parte della dottrina, risulta arduo individuare una cornice normativa entro la quale inserire tale

---

[25] A tal proposito, la prassi giurisprudenziale ha mostrato nel tempo una tendenza a rafforzare la portata applicativa della cd. *ricognizione informale*, cfr. *ex multis*, Corte appello L'Aquila, 28/05/2018, n.1269 in *Redazione Giuffrè 2018; Cassazione penale sez. IV, 13/09/2017, n.47262* in *CED Cass.* n. 271041; Cass., 29.08.2019, n. 37012 *CED Cass* n. 277635;

[26] T. Alesci, *op. cit.,* 92.

[27] Non è previsto né il diritto all'assistenza tecnica da parte del difensore né il dovere di verbalizzazione dell'atto. Cfr. T. Alesci, *op. cit*., 92. Si veda anche P. Tonini, *Manuale di procedura penale*[20], Milano 2019, 572.

[28] *Ex multis*, Cass., 25.02.2009, Pellicori e altri, in Mass. Uff., n. 243212.

[29] «Una sorta di fattispecie a formazione progressiva nell'ambito della quale il momento cruciale – quello in cui il riconoscimento avviene – è sguarnito delle garanzie che dovrebbero assicurarne la buona qualità». T. Alesci, *op. cit*., 93. Si tratta di un meccanismo che non dà alternative al pubblico ministero che intende compiere l'attività nell'immediatezza. Infatti, anche il ricorso all'incidente probatorio «nelle particolari ragioni d'urgenza» secondo quanto stabilito dall'articolo 392, comma 1, Cpp rappresenta una via non facilmente praticabile. Quest'ultima potrebbe essere intrapresa solo se «le indagini già consentono la formulazione di un giudizio di probabilità dell'identità, se l'atto può avere importanza decisiva nell'economia delle indagini, e l'accusa non possa rinunciare al dibattimento agli eventuali effetti positivi della prova in tal modo assunta». E. Fortuna, S. Dragone, E. Fassone, R. Giustozzi, *Nuovo manuale pratico del processo penale*, Padova 2002, 658.

[30] La dottrina ha individuato delle linee guida per la polizia giudiziaria nel compimento di tale attività, cfr. L. D'ambrosio, P. L. Vigna, *La pratica di polizia giudiziaria*, Padova 1998, 304 e 383.

atto atipico d'indagine[31]. Per dar seguito al riconoscimento, il soggetto verrà sottoposto alla consultazione di un album fotografico senza che il procedimento sia scandito temporalmente dall'osservanza di alcun adempimento obbligato. Nonostante l'intrinseca inaffidabilità dei suoi esiti[32], il legislatore rimane comunque consapevole della profonda influenza che le individuazioni possono svolgere nella prima fase d'indagine, essendo questa caratterizzata da ipotesi, approssimazioni e selezioni fra una moltitudine di potenziali responsabili[33].

2.1. - Entro il complesso scenario poc'anzi descritto s'innesta - dal 2017 - l'uso ordinario, da parte degli organi di Polizia, del sistema automatico di riconoscimento delle immagini (S.A.R.I.). Un tentativo di ricostruzione delle caratteristiche costitutive e operative di questo «nuovo e, per certi versi, rivoluzionario»[34] strumento può senz'altro essere operato attraverso il capitolato tecnico[35] allegato al contratto che il Ministero dell'Interno ha sottoscritto con l'azienda privata fornitrice del software[36]. Esso costituisce una delle complesse dotazioni tecnologiche a disposizione della polizia per la sorveglianza a fini di sicurezza ed un valido supporto per le attività investigative. Si basa su due algoritmi di elaborazione delle immagini che permettono di confrontare l'identità ignota di un volto raffigurato in un'immagine fotografica con quelle di milioni di soggetti foto-segnalati[37]. La procedura di comparazione permette di ridurre la cerchia dei sospettati grazie all'elaborazione di un elenco di volti selezionati e ordinati per grado di similarità (*alert*)[38]. Il sistema di intelligenza artificiale alla base del software è in grado di evidenziare le cosiddette impronte facciali (*faceprint*), ossia un certo

[31] T. Alesci, *op. cit.*, 95. Anche la Corte di Cassazione con sentenza n. 17747, 15.02.2017 ha ripercorso giuridicamente i punti controversi in tema di individuazione da parte della p.g. (si vedano anche, *ex multis,* Cass. pen., 28.02.1997, n. 3382, Falco in *CEDCass* m. 207409, Cass. pen. 1998, 1737 in *CEDCass* m. 211645, ma anche, 01.02.1996, n. 3494 in *CEDCass* m. 204956, Cass. pen., 04.02.2004 , n. 16902 in *CEDCass* m. 228043).

[32] S. Priori, *La ricognizione di persona: cosa suggerisce la ricerca psicologica*, in *DPP*, 2003, 1284; S. Priori, *La memoria di riconoscimento nell'atto di ricognizione*, in *DPP*, 2009, 775.

[33] A. Bernasconi, *Il riconoscimento fotografico curato dalla polizia giudiziaria*, in *Le indagini atipiche*, a cura di A. Scalfati, Torino 2014, 170.

[34] R. Lopez, *La rappresentazione facciale tramite software*, in *Le indagini atipiche* a cura di A Scalfati, Torino 2019, 241.

[35] Cfr. https://www.poliziadistato.it/statics/06/20160627-ct-sari--4-.pdf; https://www.poliziadistato.it/statics/17/lotto-2---sari-sistema-di-acquisizione-e-trasmissione-v23---finale--2-.pdf.

[36] Azienda leccese PARSEC 3.26 che collabora con l'Istituto di scienze applicate e sistemi intelligenti – ISASI – del Centro nazionale per le ricerche, per lo sviluppo di algoritmi di riconoscimento facciale.

[37] L'algoritmo può essere definito come un insieme di istruzioni che da un determinato *input* ricava un *output*: ricevuta la domanda, la elabora sulla base dei dati che lo costituiscono e fornisce il riscontro per cui è stato interpellato.

[38] Per un approfondimento sul funzionamento dei sistemi di riconoscimento facciale si vedano S. M.

numero di tratti, quali la posizione degli occhi, del naso, delle narici, del mento, delle orecchie, realizzando un modello biometrico finalizzato al riconoscimento (*template*)[39].

L'impiego del S.A.R.I. ha come principale obiettivo l'identificazione del soggetto ignoto la cui immagine, grazie all'estrazione del relativo *template*, viene confrontata e utilizzata come indice per la consultazione nella banca dati dei modelli biometrici di riferimento. Nel gennaio 2017, il Ministero dell'Interno attivava una procedura ad evidenza pubblica per la predisposizione di un programma di riconoscimento automatizzato[40], diretto all'attribuzione di generalità ad un soggetto ignoto sulla base di una immagine del suo volto – sia in fotografia che registrata in un *frame* ricavato da una videoripresa – processata da uno o più algoritmi di riconoscimento facciale, selezionati fra quelli testati nel 2014 dal NIST – *National Institut of Standards and Technology* – Agenzia governativa statunitense di gestione delle tecnologie[41]. Come specificatamente richiesto dal committente, il software è stato predisposto in modo da gestire due scenari operativi, l'*Enterprise* e il *Real-time*. Nella prima modalità, l'operatore ricerca l'identità di un volto statisticamente raffigurato all'interno di una banca dati di grandi dimensioni individuata nella piattaforma A.F.I.S. – S.S.A. (*Automated fingerprint identification system*), ovvero il Sistema automatizzato di identificazione delle impronte digitali integrata dal sottosistema S.S.A., contenente le foto segnaletiche dei pregiudicati, i dati anagrafici e le informazioni riguardanti i loro dati biometrici, acquisiti in sede di foto-segnalamento. L'immagine fotografica viene così filtrata e processata in pochi istanti con il volto di milioni di soggetti schedati attraverso le impronte facciali elaborate dal software.

Viceversa la modalità *real time* – finalizzata a potenziare le attività di controllo del territorio in occasione di eventi e manifestazioni – permette l'analisi automatica in tempo reale di volti ripresi in più flussi video *live* provenienti dalle telecamere installate nella medesima area. I volti presenti nei fotogrammi dei diversi *stream* video vengono comparati mediante un algoritmo di riconoscimento che attinge gli elementi della comparazione da una banca dati la cui grandezza è dell'ordine delle centinaia di

---

Smyth, *Biometrics, surveillance and the law*, New York 2019, 67; M. Tistarelli, C. Champod, *Handbook of biometrics for forensic science*, Cham 2017, 127; A. Jain, R. Bolle, S. Pankanti, *Biometrics. Personal identification in Networked Society*, New York 1999, 65.

[39] Quest'ultimo può avvenire in termini di autenticazione dell'identità: il soggetto, cioè, dichiara la propria identità e il sistema effettua un confronto "uno a uno" tra il modello biometrico rilevato e quello memorizzato; oppure in termini di identificazione biometrica e in tal caso il sistema effettua un confronto "uno a molti" tra il modello rilevato e tutti i modelli disponibili per scoprire l'identità del soggetto.

[40] Cfr. https://www.poliziadistato.it/statics/39/bozza-contratto-lotto-1-sari.pdf.

[41] Si veda https://www.nist.gov/.

migliaia di soggetti[42]. Una volta inserito il *frame*, il software "passa in rassegna" ad altissima velocità le immagini custodite in archivio e quelle ignote di provenienza eterogenea (sia catturate dallo *streaming* del video ma anche riprese da telefoni cellulari) alla ricerca di un *match*. Al termine dell'operazione, l'algoritmo restituisce una lista di profili ordinati secondo un punteggio di probabilità basato sul grado di similarità rispetto all'immagine del soggetto da individuare[43]. La corrispondenza del volto ignoto con quello schedato è resa nota all'operatore da un segnale di *alert* generato dall'algoritmo. Se la ricerca non genera alcun *alert*, l'immagine analizzata rimane memorizzata all'interno della piattaforma S.A.R.I. così da poter segnalare eventuali corrispondenze future, incrementando in tal modo la banca dati centralizzata. Se, invece, il tentativo si conclude positivamente, allora il risultato dovrà essere posto al vaglio del personale specializzato della polizia scientifica, sul quale incombe il compito di verificare l'esito elaborato dal sistema automatico. Tale fase del procedimento non costituisce, però, un rimedio in grado di rendere immune il sistema da individuazioni errate, sempre in agguato anche nei più sofisticati sistemi di reti neurali. Si ritiene che la mancanza di linee guida o *best practices* sulla qualità dell'immagine da utilizzare, sia nella sua interezza sia come fonte da cui acquisire la composizione digitale del volto, rafforzi inesorabilmente la possibilità di identificazioni poco attendibili (cfr. *supra*, nota n. 11).

2.2 Il vantaggio per il lavoro degli investigatori sul piano sia della velocità sia dell'efficienza è davvero sorprendente; basti considerare che, come sottolineato già da attenta dottrina, l'esecuzione della ricerca informatizzata in uso fino a poco meno di due anni fa, imponeva che i connotati identificativi del soggetto, dati anagrafici e somatici fossero indicati in forma descrittiva ed inseriti manualmente dall'operatore nei campi presenti nelle maschere di interrogazione[44].

Tuttavia, esistono rischi ancora molto elevati legati a questa forma di intelligenza artificiale sia per la notevole probabilità di sviluppo di risultati non attendibili, e dunque, di identificazioni errate, sia per la strumentalizzazione a fini discriminatori e di controllo politico e sociale[45], cui il suo utilizzo si presta. Nonostante ciò, dopo il primo

[42] R. Lopez, *La rappresentazione facciale tramite software*, in *Le indagini atipiche* a cura di A Scalfati, Torino 2019, 243.

[43] Relazione del Dott. L. Rinella, Direttore di Polizia Scientifica durante il convegno "*Dalle impronte digitali al riconoscimento dell'iride: il corpo umano come oggetto e mezzo di investigazione*", organizzato dall'Università del Piemonte Orientale e la Questura di Alessandria, tenutosi ad Alessandria presso il Dipartimento di Giurisprudenza e Scienze politiche, economiche e sociali in data 20 novembre 2019.

[44] Cfr. R. Lopez, *op. cit.*, 243.

[45] Il governo cinese ricorrerebbe al *face recognition* per attività di profilazione etnico-razziale nei con-

biennio applicativo di tale tecnica, i dati conosciuti sono scarsissimi[46]. Non è ancora stata resa nota l'esatta quantità dei cd. "falsi positivi" e "falsi negativi" sul totale dei risultati. Ma non è solo il costante silenzio su questi aspetti a rafforzare lo scetticismo verso l'impiego procedimentale che si dovesse eventualmente riconoscere ai suoi esiti. Vi sono molteplici e ulteriori questioni, riguardanti aspetti cruciali nel procedimento penale, che devono ancora essere risolte. Per esempio, risulta del tutto controverso lo specifico contenuto dello schedario presente all'interno di S.A.R.I. *Enterprise*, costituito da 16 milioni di volti la cui provenienza non è del tutto chiara[47]; le specifiche modalità di funzionamento del sistema[48]; la tipologia di controllo agli accessi e l'esistenza di un registro degli stessi nonché delle specifiche operazioni disposte tramite il software. Quanto più estesa risulta la zona d'ombra finora tratteggiata sull'uso di tali sistemi d'identificazione biometrica, tanto più ci si allontana da una piena compatibilità con le garanzie processuali costituzionali accordate all'indagato[49].

A ciò si aggiunge la riflessione sull'affidabilità degli esiti ottenuti da un algoritmo che risulta direttamente proporzionale alla qualità dei dati che lo "alimentano" e che

---

fronti degli Uiguri, minoranza turcofona e di fede islamica. Cfr. https://www.ilsole24ore.com/art/come-cina-usa-l-intelligenza-artificiale-controllare-uiguri-ABhvE80B. Si segnalano inoltre i rischi legati a tale forma di intelligenza artificiale non solo per l'elevata probabilità di sviluppo di risultati non attendibili e di *matches* errati, ma anche di un impiego strumentale a fini discriminatori e di controllo politico e sociale. Cfr. S. Smyth, *Biometrics, surveillance and the law. Societies of restricted access, discipline and control*, New York 2019, 138. Già nel 2011, l'Assemblea Parlamentare dell'Unione Europea nella Risoluzione 1797, affermava «*Due to its rapid development, biometric technology offers a possible solution to various security concerns, but it also puts several human rights at risk, including the right to respect for private life, the right to a fair trial and the presumption of innocence, freedom of movement and the prohibition of discrimination, as enshrined in the European Convention on Human Rights (ETS No. 5)*». In Resolution 1797, *The need for a global consideration of the human rights implications of biometrics* (http://semantic-pace.net/tools/pdf.aspx?doc=aHRocDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWY-vWDJILURXLWV4dHIuYXNwP2ZpbGVpZDoxNzk2OCZsYW5nPUVO&xsl=aHRocDovL3NlbW-FudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3OTY4). Si veda anche A. Greenfield, *Radical Technologies: The Design of Every-day Life*, New York 2017, 218.

[46] J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del garante privacy d'oltremanica)*, in *SP*, 02.2020, 20.

[47] R. Lopez, *op. cit.*, 246.

[48] Si ricorda che, aldilà di quanto descritto genericamente dal Capitolato Tecnico (vedi ut *supra*, nota n. 36), non è stato ancora dato un riscontro effettivo sul metodo di funzionamento del software e sulle modalità di apprendimento degli algoritmi posti alla base del funzionamento del S.a.r.i.

[49] R. Lopez, *op. cit.*, 239 e segg.

in quanto selezionati e immessi dall'uomo, ne mutuano i valori e il cd. *bias*[50]. La problematica non si presenta solamente nei sistemi di riconoscimento facciale, ma in ogni sistema che utilizza dati sulle persone (biometrici, comportamentali, creditizi, etc.)[51]. Pare del tutto chiara l'esigenza di una regolamentazione dei modelli biometrici utilizzati alla luce dei generali principi di *interpretability*[52] e *trasparency*[53] o, in alcuni casi,

[50] In particolare, il *bias* nei sistemi di *machine learning*, cd. "*bias* induttivo dell'algoritmo", indica la produzione di risultati con errori sistematici dovuti, per esempio, alla presenza di ipotesi di errore nel processo di apprendimento automatico. Si veda A. Greenfield, *Radical Technologies: The design of Every-day Life*, New York 2017, 218.

[51] Solitamente la presenza di *bias* nell'intelligenza artificiale è associata ad una scarsa qualità dei dati di *training*. Quest'ultima può anche presentarsi prima che i dati vengano raccolti, oppure può essere presente in altre fasi del processo di *deep learning*. Solitamente sono tre le fasi che possono dar luogo al fenomeno della "polarizzazione" dei risultati: la fase di raccolta dei dati, l'addestramento dell'algoritmo e la preparazione delle informazioni. Nei dati di *training*, il *bias* può apparire in due modalità principali: in un caso i dati raccolti non sono rappresentativi della realtà, nell'altro riflettono dei pregiudizi esistenti. Da un lato, pertanto, potrebbe verificarsi ad esempio se un algoritmo di *deep-learning* venisse alimentato con più immagini di volti dalla pelle chiara rispetto a quelli dalla pelle scura. Il sistema sarebbe meno "allenato" nel riconoscimento di soggetti aventi la pelle scura. Il secondo caso invece si presenta qualora i dati utilizzati per addestrare l'algoritmo siano presi da una serie storica provenienti da ambienti già di per sé "polarizzati" (cfr. *ut supra*). Il laboratorio *Computer Science & Artificial Intelligence Laboratory* (CSAIL) del *Massachussetts Institute of Technology* ha condotto una ricerca per dimostrare l'efficacia di un algoritmo pensato per mitigare tale indice di *bias* in un sistema di rilevamento del volto[51]. Durante il processo di *training*, l'algoritmo considera più volte dati uguali al fine di aumentare l'efficienza del calcolo e ridurre l'errore di rilevamento. L'algoritmo considerato dal laboratorio di *Computer Science & Artificial Intelligence Laboratory* (CSAIL) ha presentato una capacità di ridurre il divario presente nel rilevamento di volti caucasici e neri, seppur senza essere in grado di eliminarlo del tutto. Sul punto si veda anche J. Buolamwini, T. Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proceedings of Machine Learning Research* 81:1–15, 2018.

[52] L'interpretabilità è la qualità di un sistema di intelligenza artificiale avente ad oggetto la capacità di comprendere quali modelli vengono utilizzati per effettuare (nel caso della disciplina biometrica) identificazioni o riconoscimenti tra i soggetti. Cfr. D. V. Carvalho, E. M. Pereira, J. S. Cardoso, *Machine Learning Interpretability: A Survey on Methods and Metrics*, in *EL* 2019, 8, 10 ove, riportando una definizione di T. Miller, si afferma: «*"Interpretability is the degree to which a human can understand the cause of a decision". (...) it is important to take into consideration Electronics 2019, 8, 832 11 of 34 that when opaque machine learning models are used in research, scientific findings remain completely hidden if the model is a black box that only gives predictions without explanations*».

[53] A tal proposito, di recente il Comitato del Consiglio dei Ministri degli stati membri dell'Unione europea con Raccomandazione CM/Rec(2020)1, al punto 4.1, in materia di trasparenza ha esortato: «*States should establish appropriate levels of transparency with regard to the public procurement, use, design and basic processing criteria and methods of algorithmic systems implemented by and for them, or by private sector actors. The legislative frameworks for intellectual property or trade secrets should not preclude such transparency, nor should States or private parties seek to exploit them for this pur-*

una vera e propria limitazione dell'uso di software per il riconoscimento facciale[54], con una revisione periodica e indipendente delle reali capacità del sistema al fine di prevenire errori che possano comportare la lesione di diritti costituzionalmente garantiti.

3.- L'applicazione del S.A.R.I. è destinata ad affermarsi nel vasto filone di tecniche inedite che l'inarrestabile sviluppo scientifico degli ultimi anni ha prodotto e di cui fanno parte diversi strumenti, entro l'ampia e generica categoria delle "indagini atipiche". L'espressione evoca una nozione «sfumata»[55], forse, non così adeguata a fornire i contorni precisi di una categoria, data la pluralità delle varie attività che contiene. L'esercizio del potere investigativo conduce al compimento di diverse operazioni necessarie per assicurare le fonti di prova e quant'altro possa essere utile per la ricostruzione del fatto e per l'individuazione del colpevole.

La tendenza da parte degli inquirenti è quella di ricorrere a tali nuove metodiche di indagine non solo per l'efficacia e l'estrema velocità dei risultati, ma anche per l'indeterminatezza dei limiti che derivano all'azione investigativa. Gli aspetti concretamente coinvolti con la materia sono rappresentati dall'affidabilità del risultato, la valenza, la ripetibilità dell'atto, nonché il concreto esercizio del diritto alla difesa. È opportuno ipotizzare che l'introduzione nel processo di un sapere scientifico in continuo divenire continuerà ad arricchire il repertorio delle attività informali compiute dalla polizia, anzi, sembrerebbe che il software S.A.R.I. abbia già reso la previsione realtà, come già evidenziato di recente in dottrina[56]. Invero, la sbalorditiva efficacia pratica dello strumento sarà l'elemento determinante per decretarne l'inserimento silenzioso

pose. Transparency levels should be as high as possible and proportionate to the severity of adverse human rights impacts, including ethics labels or seals for algorithmic systems to enable users to navigate between systems. The use of algorithmic systems in decision-making processes that carry high risks to human rights should be subject to particularly high standards as regards the explainability of processes and outputs». Cfr. Committee of Ministers, *Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems*, 8 April 2020 at the 1373rd meeting of the Ministers' Deputies, https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.

[54] Cfr. C. Burt, *NIST report tackles issue of bias in facial biometrics*, disponibile su https://www.biometricupdate.com/201912/nist-report-tackles-issue-of-bias-in-facial-biometrics.

[55] Aggettivo utilizzato A. Scalfati, *Premessa* in *Le indagini atipiche*, a cura di A. Scalfati, Torino 2014, 15.

[56] «La fluidità dello scenario presente e futuro, ostaggio del "primato delle investigazioni scientifiche", impone allo studioso una sorta di "navigazione a vista", che approcciando la tecnica dell'ultima ora al riparo dalla suggestione di soluzioni preconfezionate, ne verifichi con rigore la compatibilità con il principio di legalità processuale». R. Lopez, *op.cit*., 253. Sulla nozione di "atipicità" si veda, M. Nobili, *sub. Art. 189 c.p.p.*, in M. Chiavario (a cura di), *Commento al nuovo codice di procedura penale*, tomo II, Torino 1990, 398.

tra le pratiche investigative completamente destrutturate e, quindi, fra le indagini atipiche in senso stretto (cfr. *supra*, § 3).

E', dunque, legittimo chiedersi verso quali regole processuali tenda tale forma di individuazione algoritmica. Parte della dottrina ha già cominciato a ricondurre l'applicazione di tale software alla categoria del riconoscimento fotografico curato dalla polizia giudiziaria, a sua volta prodotto atipico dell'atto di indagine di cui all'art. 361 Cpp (cfr. *supra*, § 2)[57]. Ciò che cambia in modo ineludibile è la natura del ricognitore: in un caso "un programma" nell'altro l'"uomo". Nonostante un'iniziale diffidenza verso un metodo di tal genere, la prassi e l'esperienza potrebbero condurre a dimostrare che l'attività di ricognizione automatica superi per affidabilità di esiti quella tradizionale riservata alla capacità mnesica dell'uomo che, da tempo la scienza psicologica considera un metodo del tutto inaffidabile (cfr. *supra*, § 2). Tuttavia, solo osservando e costruendo tali software secondo precise *practices*[58] e avendo come guida il principio di *interpretability*[59], sarà possibile applicare forme di intelligenza artificiali che aspirino ad essere attendibili[60]. Il S.A.R.I., ad oggi, sembra non offrire garanzie credibili sul piano della conformità alle «significative precauzioni metodologiche»[61] che l'Unione europea esorta ad adottare per assicurare la trasparenza, qualità e verificabilità esterne delle procedure utilizzate[62]. L'attività di falsificazione e ripetizione del riconoscimento

[57] R. Lopez, *op. cit*,, 253.

[58] Sul punto, anche S. Marcolini, insiste per una riforma legislativa o l'introduzione di linee guida in grado di guidare gli operatori nel corretto uso della tecnologia in fase di indagini preliminari, cfr. S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta* in *CP* 2/2015, 760 e segg. In particolare, i punti cardine da seguire sono il rispetto dei diritti fondamentali, il divieto di discriminazione, la trasparenza, l'imparzialità, la garanzia di qualità e sicurezza dei dati, la comprensibilità, la verificabilità e le garanzie di controllo da parte dell'utente. Alcuni di questi aspetti sono stati oggetto di una recente Raccomandazione da parte del Comitato dei Ministri del Consiglio d'Europa, CM/Rec (2020)1. V. Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies), https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a09e1154.

[59] Cfr. *supra*, § 2.2.

[60] S. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in www.lalegislazionepenale.eu, 18 dicembre 2018, 3-4. Sui possibili rimedi alle problematiche connesse all'utilizzo di software automatici si veda S. Quattrocolo, *Equita' del processo penale e* automated evidence *alla luce della convenzione europea dei diritti dell'uomo*, in *RÍEDP*, Vol. 2/2019, 14-15.

[61] S. Quattrocolo, *Intelligenza artificiale e giustizia*, *op. cit*., 8.

[62] «Le *chances* per contrastare l'individuazione dell'indagato quale esito di una analisi che, per sue caratteristiche intrinseche, è inaccessibile, paiono realisticamente esigue per la difesa; ed anche la nomina di un consulente tecnico per confutare la certificazione dell'output da parte della polizia scientifica, in particolare quando la corrispondenza tra i volti comparati sia espressa per grado di similarità,

operato attraverso l'algoritmo risulta ancora preclusa alla difesa in tale ambito, impedendo di fatto ogni possibilità di contraddittorio sullo specifico funzionamento del software considerato[63].

4. – L'utilizzo della tecnologia di *automated facial recognition*, come altre, è ricco di insidie, a maggior ragione se si considera la natura della disciplina biometrica tipicamente statistico-probabilistica. L'introduzione sistematica delle summenzionate tecnologie biometriche all'interno del processo penale, porta con sé problematiche in termini di affidabilità dei risultati scaturenti dalla loro applicazione e di compatibilità fra le disciplina in esame e le tradizionali categorie del processo penale. In generale, i dati biometrici devono essere analizzati e valutati in termini di "accuratezza scientifica" e si deve caso per caso comprendere quale tipo di "valore" probatorio accordare loro, alla luce dei requisiti di trasparenza, robustezza e tracciabilità di cui devono essere dotati i sistemi. Il rischio è che una scarsa comprensione delle nuove tecnologie conduca irrimediabilmente a rischi e derive inquisitorie. A fronte delle numerose incertezze interpretative e delle obiettive difficoltà applicative delle tradizionali categorie processuali penali a strumenti automatici di riconoscimento facciale, l'unica certezza sembra essere rappresentata da un grado di affidabilità troppo debole, in quanto esito di una procedura ancora "oscura" e di dati ancora ignoti alla difesa[64].

non risultando *icto oculi* attendibile o inattendibile, sconta il vizio d'origine di una individuazione che per scaturire da una tecnologia automatizzata, esercita una suggestione sull'operatore, probabilmente poco restio ad abbandonare l'ipotesi del software». R. Lopez, *op. cit.*, 256-257.

[63] Un confronto può esserci solo sulla relazione della polizia scientifica illustrativa del grado di affidabilità del risultato, attraverso parametri identificativi metrici e fisionomici. Si ricorda che «L'importante è che la prova scientifica, nel momento in cui entra nel processo penale, ne rispetti (...) le fondamentali regole, rappresentate, per quanto riguarda la formazione della prova, dal contraddittorio e, per quanto riguarda la valutazione, dall'esigenza che il sapere altamente specialistico, veicolato dalla prova scientifica, sia reso pienamente accessibile al giudice come alle parti, pena il rischio che, altrimenti, la sentenza si riduca alla mera recezione di scelte altrove deliberate». P. Ferrua, *Presentazione*, in G. Carlizzi, G. Tuzet (a cura di), *La prova scientifica nel processo penale*, Torino 2018, 5.

[64] Cfr. R. Lopez, *op. cit.*, 257.