HISTORY
LAW &
LEGAL
HISTORY

120 ANNI DI POLIZIA SCIENTIFICA: L'IDENTIFICAZIONE PERSONALE TRA SCIENZA E DIRITTO

ATTI DEL CONVEGNO
(Palermo, 18-19 aprile 2023)

a cura di
Paola Di Simone, Annalisa Mangiaracina
e Lucia Parlato

PANORMITANÆ
PALERMO
UNIVERSITY
PRESS

HISTORY
LAW &
LEGAL
HISTORY

120 ANNI DI POLIZIA SCIENTIFICA: L'IDENTIFICAZIONE PERSONALE TRA SCIENZA E DIRITTO

ATTI DEL CONVEGNO

(Palermo, 18-19 aprile 2023)

a cura di
Paola Di Simone,
Annalisa Mangiaracina
e Lucia Parlato

HJLH HISTORY LAW & LEGAL HISTORY

HISTORY, LAW & LEGAL HISTORY - 17

120 ANNI DI POLIZIA SCIENTIFICA: L'IDENTIFICAZIONE PERSONALE TRA SCIENZA E DIRITTO
a cura di Paola Di Simone, Annalisa Mangiaracina e Lucia Parlato

E-mail: hllh@unipa.it

ISSN: 2724-4857
ISBN stampa: 978-88-5509-795-6
ISBN online: 978-88-5509-798-7

Via Serradifalco, 78
90145 Palermo - Italia
www.newdigitalfrontiers.com

PALERMO UNIVERSITY PRESS

INDICE GENERALE

NOTA DELLE CURATRICI

Il 18 e 19 aprile 2023, presso l'Aula magna del Dipartimento di Giurisprudenza dell'Università degli Studi di Palermo, si è tenuto un Convegno, suddiviso in due sessioni, per celebrare i 120 anni dalla nascita della Polizia Scientifica, organo sempre più protagonista durante la fase delle indagini preliminari in ambito penale. L'incontro – promosso dal Gabinetto Regionale di Polizia Scientifica e supportato dal Dipartimento di Giurisprudenza – si è caratterizzato per la partecipazione, in qualità di relatori, di esperti della Polizia Scientifica, magistrati, avvocati e docenti universitari.

Nel corso della prima sessione, dedicata alla "Prova del DNA nel processo penale", dopo un coinvolgente e 'immaginario' dialogo tra il Dott. Pasquale Alongi, Dirigente del Gabinetto Regionale della Polizia Scientifica di Catania e il Prof. Salvatore Ottolenghi, fondatore della Scuola di Polizia Scientifica, hanno preso la parola la Dott.ssa Paola Di Simone, Direttore tecnico superiore della Polizia di Stato, la Dott. ssa Luisa Bettiol, sostituto procuratore della Repubblica presso il Tribunale di Palermo e l'Avv. Antonino Reina, del Foro di Palermo. Gli interventi hanno sottolineato il ruolo che le tecniche di identificazione fondate sull'impronta genetica, il cd. DNA *fingerprint* – sviluppatesi nel 1984 – continuano ad assumere all'interno delle dinamiche del procedimento penale, non senza però segnalare le 'ombre' che si addensano sul versante dei diritti della difesa, anche in considerazione di alcuni orientamenti giurisprudenziali.

La seconda sessione, intitolata "Dalle impronte digitali al riconoscimento facciale", ha ricostruito, in chiave prima scientifica e poi giuridica, il lungo percorso che ha condotto alle nuove tecniche di identificazione, fondate, appunto, sul riconoscimento facciale degli individui: tema, quest'ultimo, oggetto di ampio dibattito, talvolta in chiave critica, nella comunità tutta, anche a livello sovranazionale. Nel corso della sessione sono intervenuti il Dott. Stefano Sorrentino, Vice Questore della Polizia di Stato, il Dott. Massimo Taormina, Ispettore della Polizia di Stato, il Dott. Giovanni Tessitore, Direttore tecnico capo della Polizia di Stato, le Prof. Annalisa Mangiaracina e Lucia Parlato, entrambe del Dipartimento di

Giurisprudenza, il Dott. Pierangelo Padova, sostituto procuratore della Repubblica presso il Tribunale di Palermo e l'Avv. Massimo Motisi, del Foro di Palermo.

IL RICONOSCIMENTO FACCIALE: VANTAGGI E INSIDIE ALLA LUCE DELLA GIURISPRUDENZA DELLA CORTE EDU

Lucia Parlato
Università degli Studi di Palermo

Abstract: Facial recognition is currently placed at the centre of a lively 'multilevel' debate. The increasing use of this tool by judicial authorities has clear advantages as well as weaknesses. The paper aims to highlight this complicated scenario, having regard to supranational sources and – in particular – ECtHR judgements, in order to seek a suitable balance between investigative needs and individual rights protection.

Parole chiave: riconoscimento facciale; indagini atipiche; garanzie individuali; CEDU; Corte di Strasburgo.

1. Intelligenza artificiale e SARI: tra sviluppo delle tecniche investigative e impulsi sovranazionali

L'uso dell'intelligenza artificiale nel contesto del procedimento penale è sempre più diffuso e pesa in maniera crescente sugli esiti processuali. Un avanzato sistema tecnologico risulta capace, oggi, di offrire prestazioni assimilabili per molti versi a quelle dell'intelligenza umana, vantando 'competenze' che possono porsi a servizio dell'accertamento giudiziario in una svariata serie di modi.

Un versante specifico è quello inerente al cd. riconoscimento facciale, la cui utilità ha assunto particolare risalto, specie nella fase investigativa. Qualche breve considerazione introduttiva consente di notare come si tratti di una procedura comparativa che rileva e paragona le cd. impronte facciali (*faceprints*), valorizzando la corrispondenza di un certo numero di tratti somatici (come, ad esempio, la posizione di occhi, naso e mento, o la distanza tra loro).

Al di là di un complesso insieme di aspetti tecnici che non può essere qui esplorato, un semplice cenno al funzionamento del sistema mira a evidenziare come – nel corso dell'accertamento di reati – due algoritmi servano a circoscrivere la cerchia delle persone da ritenere sospettate. Questo

obiettivo si persegue tramite l'elaborazione di un elenco di volti selezionati e posti in ordine secondo un grado di similarità, rispetto a un modello dal quale prende le mosse l'indagine, se non persino attraverso l'individuazione di un volto perfettamente sovrapponibile al modello stesso.[1]

Provando a semplificare un contesto articolato, è possibile ricondurre a un'approssimativa bipartizione le molte varianti offerte dalla tecnologia, a fronte di una verifica biometrica. Un primo metodo implica un confronto 'uno a uno', grazie a un punto di partenza rappresentato dall'identità di un soggetto nota – se non da lui dichiarata –, dalla quale prende le mosse il confronto in questione. Un'altra tecnica, invece, si basa su un'identificazione biometrica da 'uno a molti' e tende a scoprire l'identità di un individuo ignoto attraverso il raffronto con numerosi modelli disponibili.

La seconda tra le due procedure è quella maggiormente utile alle indagini e, al contempo, la più controversa. A essa si riconduce il sistema automatico di riconoscimento delle immagini – cd. SARI –, da diversi anni disponibile per la polizia di Stato, che mira all'identificazione biometrica di uno sconosciuto.[2] Il primo passo qui è l'estrazione del modello biometrico di quest'ultimo soggetto, la cui immagine viene comparata con gli esemplari contenuti in una banca dati che raccoglie una moltitudine di modelli biometrici di riferimento. In concreto, accade sovente che sulla scena del crimine si possa reperire una quantità limitata di elementi, tra i quali spiccano quelli riferibili a una persona, colti grazie alle telecamere presenti sul posto. Una selezione tra i fotogrammi più fruibili a seconda della loro definizione, chiarezza e angolazione, può consentire una comparazione tra i connotati ricavati e i volti 'schedati' nella piattaforma SARI. A valle di questa scrematura, attività successive sono orientate verso la ricerca e l'individuazione di soggetti potenzialmente in grado di fornire circostanze utili per la ricostruzione dei fatti. È evidente come il nucleo di circostanze che più condiziona la fruttuosità di questo *iter* si collochi al suo avvio, consistendo nella reperibilità e qualità di elementi a disposizione ai fini di questa verifica.

1 Cfr. Lopez 2019: 241; Colacurci 2022.

2 In proposito si rinvia alle ampie considerazioni di A. Mangiaracina, *supra*, in questo volume.

Nel contesto delle operazioni appena riportate, emergono varie possibili opzioni. Soprattutto, una differenza di fondo distanzia due modalità investigative che fanno riferimento rispettivamente a 'campionari' di natura profondamente diversa. Da un canto, il sistema SARI cd. *enterprise* rimanda a un'ampia risorsa di 'volti', almeno sedici milioni di unità, la cui provenienza non risulta del tutto chiara o univoca.[3] Dall'altro canto, il sistema SARI cd. *realtime* confronta il modello facciale dal quale l'indagine prende avvio con quelli afferenti a una serie indefinita di individui: i loro connotati vengono colti 'in movimento' grazie al posizionamento di telecamere in luoghi pubblici considerati cruciali ai fini investigativi.

La seconda tra le due forme appena indicate è quella per cui si accentuano gli interrogativi e i timori che di per sé contrassegnano l'ambito qui esaminato. Essa suscita maggiori preoccupazioni anche per le insidie dovute sovente alle connotazioni poco chiare dei volti esaminati, nonché per i rischi di eccessiva ingerenza nella sfera delle garanzie individuali di chi sia coinvolto, anche a propria insaputa, nel raggio di captazioni svolte in maniera diffusa.

Le distanze tra i due modelli sono oggetto di una consapevolezza crescente all'interno delle fonti dell'Unione europea, la cui evoluzione ha preso le mosse dal cd. GDPR, del 2016,[4] e dalla Direttiva 2016/680/UE. Incidentalmente, va rammentato come in materia rilevi altresì la Dichiarazione 21 allegata al Trattato di Lisbona in tema di protezione dei dati personali nel settore della cooperazione giudiziaria e di polizia in materia penale, nonché la previsione di cui all'art. 8 della Carta dei diritti fondamentali dell'Unione europea. Ma, tornando al dualismo che percorre le modalità del riconoscimento facciale, non si può trascurare come esso sia emerso nitidamente all'interno del dialogo 'a tre' che ha impegnato la Commissione europea, il Consiglio e il Parlamento, ai fini dell'adozione di una fonte normativa volta a regolare l'uso della cd. intelligenza artificiale. I rispettivi approcci si sono ri-

3 Lopez 2019: 240.

4 Regolamento dell'Unione europea 27 aprile 2016, n. 679 (v. art. 4, comma 14), attuato in Italia con d.lgs. 10 agosto 2018, n. 101; Direttiva 2016/680/UE, del Parlamento europeo e del Consiglio, del 27 aprile 2016 (nota anche come LED, *Law Enforcement Directive*), recepita in Italia con d.lgs. 18 maggio 2018, n. 51.

velati divergenti, ma con una costante rappresentata dall'attenzione per le differenze tra i due tipi di attività definite come riconoscimento facciale *enterprise* e *realtime*. Attenzione che costituisce una cifra evidente all'interno del testo formulato, cd. regolamento sull'intelligenza artificiale, e, in particolare, del suo art. 5 che limita fortemente l'uso del sistema di identificazione biometrica remota "in tempo reale".[5]

Ciò posto, ci si soffermerà di seguito su alcuni aspetti concernenti la delicata qualificazione della fattispecie del riconoscimento facciale, per affrontare poi i principali profili presi in considerazione dalla giurisprudenza della Corte di Strasburgo e riscontrare il loro impatto sull'evoluzione del dibattito e delle fonti normative in materia.

2. Il difficile inquadramento della fattispecie

Di fronte a una fattispecie così innovativa, è naturale che sorgano interrogativi quanto al suo inquadramento sistematico e alla sua compatibilità con le garanzie costituzionali assicurate all'individuo in relazione allo svolgimento di attività giudiziarie.

L'assenza di specifici riferimenti normativi induce a ricondurre lo strumento del riconoscimento facciale all'alveo delle 'indagini atipiche'. Si tratta di una formula generica che evoca una 'nozione sfumata', non in grado di delineare i contorni precisi di una categoria.[6]

La norma che fa riferimento a questo contesto è tra quelle che, all'interno del codice di procedura penale, aprono più incertezze. Nel fare richiamo a 'prove atipiche' e non ad attività di indagine, l'art. 189 c.p.p. fissa presupposti non agevolmente mutuabili nella fase iniziale del procedimento penale: soprattutto laddove richiede un contraddittorio tra le parti inerente alle modalità da adottare nello svolgimento delle attività istruttorie. Questo aspetto è talmente critico che la

5 Regolamento 1689/2024 del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

6 Scalfati 2014: XV ss.

dottrina, nell'evidenziarlo, ha talvolta auspicato l'introduzione nel codice di rito di un articolo *ad hoc* (art. 189-*bis* c.p.p.) che, inserito dopo quello citato, possa costituirne il *pendant* dedicato alla fase delle indagini preliminari.[7]

Lo svolgimento delle attività di riconoscimento facciale finisce ad ogni modo, in concreto, per arricchire il catalogo di attività informali di polizia, assumendo una posizione centrale tra le investigazioni di carattere scientifico e tecnologico. Come accade di consueto di fronte a operazioni investigative innovative e sprovviste di un preciso appiglio normativo, sorge il dubbio che il suddetto riconoscimento possa rappresentare una semplice modalità rivisitata e moderna, rispetto ad attività già esistenti e regolate dal legislatore. La circostanza che un simile quesito sorga di frequente in relazione a indagini tecnologicamente avanzate svela un'incertezza di fondo. Riguarda l'individuazione della soglia oltre la quale un *quid* inedito riesca a qualificare un autonomo e ulteriore strumento investigativo e non soltanto semplici metodologie esecutive di atti investigativi già noti al sistema. Sinora, i principali dubbi hanno riguardato le varie possibilità investigative che 'gravitano' attorno al nucleo originario dell'istituto delle intercettazioni, specie in relazione all'uso di tabulati,[8] ma soprattutto con riguardo all'impiego del *trojan*.[9] Senza contare le difficoltà poste dall'utilizzo del cd. gps, considerato poi come una forma innovativa di pedinamento.[10]

In quest'ottica, ricercando rapporti di equivalenza funzionale, il riconoscimento facciale potrebbe essere accostato al riconoscimento fotografico tradizionale, individuando il discrimine tra i due contesti soprattutto nella natura del 'ricognitore', rispettivamente una macchina o un uomo. Dotato di una memoria considerata più fallace, quest'ultimo può risultare meno affidabile a paragone con un sistema artifi-

7 Marcolini 2010: 2855 ss.; Marcolini 2015: 760 ss.

8 I punti più salienti di un intenso *excursus* coincidono con Cass., Sez. un., 23.2.2000, n. 6, D'Amuri, Rv. 215841; Corte cost. 7 luglio 1998, n. 281; 26 maggio 2010, n. 188; 23 gennaio.2019, n.38; Corte giust., 2 marzo 2021, causa C-746/18, Prokuratuur; D.L. n. 132 del 30 settembre 2021 conv. in l. legge 23 novembre 2021, n. 178.

9 Tra le altre, Cass., Sez. V, 30 settembre 2020, n. 31604-20, in ordine all'uso del trojan come 'modalità' di captazione, nel contesto di un dibattito vivace e esteso.

10 Tra le molte, Cass., Sez. II, 13 febbraio 2013, B., Rv. 255542.

ciale, capace di cogliere uno scatto e un attimo in modo da cristallizzare l'immagine.[11]

In questa prospettiva, il riconoscimento facciale nascerebbe come 'una costola' di quello fotografico curato autonomamente dalla polizia giudiziaria, il quale costituirebbe a sua volta una discendenza atipica rispetto all'atto omologo del mezzo di prova della ricognizione.[12] Passaggio, quello appena indicato, che può essere percorso facendo richiamo all'art. 361 c.p.p., in base al quale "quando è necessario per la immediata prosecuzione delle indagini, il p.m. procede alla individuazione di persone" presenti fisicamente o ritratte in immagini sottoposte a chi deve eseguire l'individuazione. Alla libertà nelle forme di tale riconoscimento, cui non corrisponde la redazione di un verbale, si accompagnano conseguenze di segno diverso tra loro connesse. In particolare, da un lato la mancanza di un'esplicita valenza probatoria, dall'altro una flessione delle garanzie tale da consentire che l'atto sia compiuto senza la partecipazione del difensore.

Da considerare separatamente, anche per le sue implicazioni rispetto alla tutela delle garanzie individuali, è l'ipotesi di utilizzo di sistemi di riconoscimento facciale, al fine dello sblocco di un dispositivo elettronico. Ci si riferirà a questo aspetto soltanto brevemente, con i rapidi cenni inseriti qui di seguito. Un problema specifico, da menzionare, si ricollega all'utilizzo di questa tipologia di 'chiavi di accesso' nel corso di attività investigative e, ancora più in particolare, alla possibile richiesta rivolta alle persone indagate dalle autorità inquirenti di abilitare le forze dell'ordine all'utilizzo del *device*. Le questioni più interessanti, che sorgono già in relazione a una simile richiesta delle stesse autorità, volta a ottenere semplici *password*,[13] si ripropongono con riguardo ai filtri di accesso più moderni, basati sulla rilevazione dei connotati dell'utente. Corrispondenti per un nucleo comune, le due situazioni inducono l'interprete a interrogarsi sul possibile affermarsi di una declinazione del diritto di difesa che valga a sgravare l'indagato dall'obbligo di rivelazione delle *password* o di tenere comportamenti che consentano lo sblocco in questione. Il punto centrale

11 Lopez 2019: 240 s.

12 Tra gli altri, Dalia-Ferraioli 2016: 352; Lopez 2019: 253.

13 Volendo, Parlato 2020: 291 ss.

ruota attorno alla possibile configurabilità di un'ipotesi di diritto al silenzio e sulla prospettabilità di un rifiuto che valga a sottrarre la persona interessata dall'esporre i propri connotati a una posizione che consenta di sbloccare il dispositivo. Questo aspetto, non regolato in Italia e in molti Paesi, in Germania è previsto dal § 81b StPO, parzialmente censurato dalla Corte costituzionale per escludere la acquisizione coattiva di una sommatoria di dati biometrici.[14] Mentre, sulla scorta del dato normativo una pronuncia ha ammesso lo sblocco coercitivo del *device*, realizzato avvicinando coattivamente al dispositivo il volto del suo proprietario, o la mano per sfruttare le impronte digitali.[15] Di questo aspetto si è occupata una proposta di matrice accademica, limitando l'uso di coercizione fisica per ottenere dati biometrici.[16]

3. Una rete intricata di vizi e virtù

Nonostante le sue risultanze possano rivelarsi meno affidabili di quanto appaia a prima vista, il riconoscimento facciale finisce per assumere un'importanza considerevole nel rito penale, soprattutto in coincidenza con i passi iniziali delle indagini. Offre prestazioni particolarmente promettenti, in chiave investigativa, anche per la rapidità con cui il *software* utilizzato processa le immagini che gli vengono sottoposte.[17]

La fulminante efficacia pratica dello strumento[18] imprime ritmi veloci, molto allettanti soprattutto nell'immediatezza della commissione di gravi fatti criminosi. Esso è capace, infatti, di realizzare rapidamente una prima selezione di massima tra le persone sospettabili, o in grado di riferire circostanze utili. Il momento appena successivo all'emersione della notizia di reato, tuttavia, è delicatissimo, in quanto certe piste investigative – se scartate automaticamente in

14 BVerfG, 29.7.2022, 2 BvR 54/22.

15 LG Ravensburg 14 febbraio 2023.

16 Art. 9, *Proposal for a Directive of the EP and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings* (ELI Proposal), 2023.

17 Lopez 2019: 250.

18 Scalfati 2011: 144.

questo frangente – rischiano di restare in seguito definitivamente inesplorate. Potrebbero rivelarsi proficue solo successivamente, quando molti elementi istruttori risulterebbero oramai dispersi.

Margini di errore nell'uso del riconoscimento facciale possono dipendere da svariate ragioni. Gli sbagli più temibili sono da addebitare al cd. pregiudizio dell'algoritmo. Il numero più elevato di 'falsi positivi', infatti, si registra in relazione a persone di etnie o genere diversi da quelli cui è riconducibile la quantità maggiore di immagini incluse nella banca dati di riferimento. Una simile predisposizione alla fallacia, di solito, si presenta più accentuata in svantaggio delle donne con la pelle scura, mentre di rado riguarda uomini di pelle chiara. Ciò dipende dai 'modelli' in base ai quali l'algoritmo viene in prevalenza alimentato e 'allenato'. Ne deriva che il livello di attendibilità di un sistema risulta proporzionale al grado di 'neutralità' della raccolta di dati che 'nutre' il sistema stesso.

Non mancano altre tipologie di possibili disfunzioni, originate da difetti di chiarezza o definizione dell'immagine o del dato che si va a raffrontare, di volta in volta, nel contesto delle operazioni di comparazione e riconoscimento. Pur in presenza di simili anomalie ravvisabili all'origine dell'atto investigativo, può verificarsi che – non essendo in possesso di altri elementi istruttori – le forze dell'ordine scelgano comunque di attivare le procedure di riconoscimento, interpellando il sistema. In queste situazioni, dovrebbe comunque tenersi conto del riscontrato difetto di partenza, in modo da evitare che l'intera indagine rischi di essere compromessa, rivolta esclusivamente verso alcune direzioni ed erroneamente priva di attenzione per altre strade investigative. Rispetto a questa tipologia di disfunzioni, in definitiva, si giunge a confidare sul ruolo e sull'esperienza dell'operatore, scaricando così una significativa dose di responsabilità sull' 'uomo', a valle rispetto alla delicata sequenza tecnologica. Ne deriva che – quantomeno finché non saranno disponibili parametri normativi ben precisi – risulta auspicabile la creazione e la circolazione di protocolli in grado di fornire precise indicazioni, da seguire sin dalla selezione dell'immagine originale e nell'intero corso della procedura svolta tramite l'intelligenza artificiale.[19]

19 Lopez 2019: 248.

Quanto alla sua paternità, la procedura tendeva in origine a ricadere in un contesto gestito più direttamente dal pubblico ministero. Nello sviluppo della prassi, tuttavia, essa è gradualmente passata nelle mani della polizia giudiziaria, autorizzata a indirizzare di propria iniziativa lo svolgimento di operazioni di individuazione fotografica in gran parte accomunate a quelle del p.m., specie per la libertà delle forme, la documentazione sintetica e la mancanza di assistenza difensiva.

Il rilievo dell'atto, dotato di caratteristiche peculiari che ne esaltano anche la non ripetibilità, è capace di proiettarsi in svariati ambiti del procedimento penale. Senz'altro tale rilievo si ripercuote sulle valutazioni in materia cautelare,[20] nonché nel corso del giudizio abbreviato,[21] oltre che in sede di udienza preliminare.[22] A ciò si aggiunge che, peraltro, con riguardo alla fase dibattimentale, la Corte di cassazione – anziché ritenere sempre necessario l'apporto del ricognitore nello svolgimento dell'attività probatoria di cui agli artt. 213 e 214 c.p.p. – in varie ipotesi tende ad ammettere che il riconoscimento possa essere veicolato attraverso i meccanismi delle contestazioni e delle letture, ovvero tramite la testimonianza indiretta dell'ufficiale di polizia giudiziaria in ordine all'individuazione svoltasi in sua presenza.[23]

Spostando lo sguardo verso le garanzie costituzionali, ci si accorge che tutto ciò può tradursi in una discrasia con il principio del contraddittorio di cui all'art. 111 Cost., determinando un sacrificio del diritto di difesa garantito dall'art. 24 Cost. Le risultanze istruttorie raccolte, in sostanza, possono difficilmente essere poste in discussione. Anzi, la loro incidenza può essere tale da far vacillare il rispetto della presunzione di innocenza, sancito dall'art. 27 Cost., divenendo capace di sovvertire la distribuzione dell'onere probatorio. Quest'ultimo, infatti, in concreto può finire per virare e porsi a carico della persona sottoposta al procedimento penale, chiamata a dimostrare – ad esempio – che non si trovava in un determinato luogo in un certo momento, oppure – con ancora mag-

20 Cass., Sez. II, 16 febbraio 2015, n. 6505, Fiorillo, Rv 262599.

21 Cass., Sez. VI, 11 aprile 2007, n. 18459, Rv. 236420.

22 Cass., Sez. III, 2 agosto 1993, n. 1751, Beltrame, Rv. 194474.

23 In questo senso, tra le altre, Cass., Sez. II, 2 ottobre 2015, n. 43294, Ahmetovic, Rv. 265078.

giori difficoltà – che la propria identificazione e localizzazione è stata effettuata, da parte degli inquirenti, proprio grazie a metodi investigativi non ammessi dall'ordinamento.

Tutto ciò senza contare la spiccata ingerenza delle operazioni in questione – rispetto alla sfera privata della persona, tutelata a livello costituzionale – non solo in relazione a chi sia sottoposto al procedimento penale, ma anche con riguardo a una serie indefinita di soggetti 'terzi' che entrino, anche a loro insaputa, nel raggio di azione delle attività di riconoscimento e di quelle prodromiche.

4. La giurisprudenza della Corte EDU: due ordini di pronunce

Dinanzi all'utilizzo dello strumento del riconoscimento facciale, si affacciano problematiche concernenti il rispetto di alcune norme della CEDU, in particolare, degli artt. 6 e 8. Al riguardo, trovandoci di fronte a un istituto complesso che determina sia aspirazioni che timori, occorre operare un bilanciamento tenendo conto delle esigenze investigative e, al contempo, della tutela di diritti fondamentali di diversa natura.

Da un esame della giurisprudenza della Corte EDU, i principali profili di interesse emergono soprattutto da due gruppi di sentenze. Interessano, da un canto, più genericamente, questioni relative alle garanzie individuali, a fronte dell'utilizzo di certe tecniche investigative; dall'altro, in maniera più mirata, problematiche concernenti l'argomento qui trattato. In aggiunta rispetto ai suddetti ambiti giurisprudenziali, si intende rivolgere l'attenzione in maniera autonoma verso un ultimo provvedimento, tra i più recenti in materia.

4.1. Il rapporto controverso tra tecnologia e accertamento penale

Un primo ordine di pronunce assume importanza nell'analisi della fattispecie del riconoscimento facciale, pur non coinvolgendola direttamente. Nel contesto di un panorama assai ampio, è possibile enucleare alcuni casi emblematici. Le

tre sentenze sotto selezionate rappresentano spunti utili per mostrare come, davanti all'uso della tecnologia nell'accertamento giudiziario, la Corte si sia trovata a constatare la tensione esistente tra esigenze sia istruttorie che di tutela dei diritti fondamentali.

Una pronuncia da menzionare, anzitutto, è quella inerente al 'caso *Sigundur Einarsson c. Islanda*', del 2019,[24] nel quale era emerso come l'organo dell'accusa avesse operato tramite algoritmi, per ottenere una scrematura del materiale raccolto nel corso di investigazioni svolte ad ampio raggio. Il sistema, denominato '*Clearwell*', lavorava su parole-chiave capaci di produrre una selezione di documenti. Attraverso tre separate ricerche erano stati formati dei 'contenitori' di materiali selezionati, 'taggati' e contrassegnati da rispettivi nomi. Le risultanze suddivise in questo modo erano state manualmente ripercorse dagli inquirenti e i soli elementi così filtrati erano stati posti a disposizione dei difensori dell'accusato.

L'esito della valutazione della Corte avrebbe potuto influire su un esteso novero di procedimenti affetti da prassi simili. Questo potenziale effetto non ha avuto luogo, tuttavia, in quanto una violazione dell'art. 6 CEDU è stata riconosciuta, ma è stata imputata a un aspetto del tutto diverso, anch'esso lamentato dal ricorrente. Inerente a un difetto di imparzialità del giudice, tale aspetto ha avuto valore assorbente rispetto alla considerazione del profilo derivante dall'uso dell'algoritmo, non reputato meritevole di essere oggetto di una condanna dello Stato interessato.

Va messa in risalto, però, l'opinione parzialmente dissenziente espressa da un giudice della Corte europea,[25] il quale ha manifestato il proprio disaccordo rispetto al mancato riscontro di una violazione dell'art. 6 CEDU per il presunto diniego di accesso della difesa ai dati investigativi. Il giudice ha inteso sottolineare come l'art. 6 par. 1 e 3 (b) CEDU renda doverosa una *discovery* che abbracci l'insieme dei materiali investigativi, comprensivo di eventuali prove a discarico.[26] Ha evidenziato, in particolare, i diritti della difesa – di acces-

24 Corte EDU, 4 giugno 2019, *Sigurður Einarsson e altri c. Islanda*.

25 V. opinione parzialmente dissenziente espressa dal giudice dal giudice D. Pavli.

26 Corte EDU, 23 maggio 2017, *Van Wesenbeeck c. Belgio*; 31 marzo 2009, *Natunen c. Finlandia*.

so e divulgazione rispetto alle prove raccolte dall'accusa – per specificare che ogni sacrificio di tali diritti debba essere 'strettamente necessario', in considerazione della parità delle armi sottesa al disposto dell'art. 6 CEDU,[27] segnalando altresì come l'autorità giudiziaria nazionale abbia mancato di svolgere un'adeguata verifica in ordine a questo aspetto. Ciò posto, sempre secondo l'opinione citata, emerge come la pronuncia della Corte EDU abbia aggirato un problema di rilievo, lasciandosi sfuggire l'occasione per affrontare la materia delicata concernente il rapporto tra nuove tecnologie e diritti della difesa in punto di prova.

Una seconda sentenza, afferente a questo primo nucleo giurisprudenziale, che interessa solo in via mediata il tema qui trattato, riguarda il caso *B.S. c. Spagna*.[28] Incentrata sul cd. *phenotyping* e su profili di discriminazione, la pronuncia assume rilievo in ordine al problema relativo al cd. pregiudizio algoritmico. Basti ricordare che la fattispecie riguardava la lamentata violazione dell'art. 3 CEDU, in quanto la ricorrente affermava di essere stata vittima di abusi realizzati sia verbalmente che fisicamente, da parte delle forze dell'ordine che l'avevano fermata e interrogata. Le condotte pregiudizievoli sarebbero state sofferte dalla donna a causa del genere femminile, ma soprattutto del colore della pelle. Secondo quanto la stessa riportava, altre donne – come lei coinvolte in un sospettato giro di prostituzione, ma di pelle bianca – non erano state destinatarie di un simile trattamento. Sempre la ricorrente, peraltro, si doleva del linguaggio usato dal giudice nazionale che, in un provvedimento, aveva fatto riferimento a un "vergognoso spettacolo della prostituzione sulla pubblica via". Sulla scorta dell'art. 3 CEDU, nel ricorso alla Corte EDU si sottolineava l'inadeguatezza dell'indagine giudiziaria condotta a livello nazionale in seguito alla denuncia proposta dalla signora. Nel riscontrare non soltanto il vizio relativo alla norma appena richiamata, ma anche la violazione dell'art. 14 CEDU, quanto alla discriminazione indicata, la Corte EDU si è espressa riconoscendo l'inosservanza degli obblighi procedurali positivi a carico degli Stati, sulla falsariga di pronunce precedenti.

27 Corte EDU, 23 maggio 2017, *Van Wesenbeeck c. Belgio*, § 68.

28 Corte EDU, 24 luglio 2012, *B.S. c. Spagna*.

Un'ulteriore presa di posizione da ricordare, proprio per il riferimento agli obblighi appena menzionati, riguarda il caso *Y. c. Bulgaria*, in cui la Corte europea – nel valutare la presenza di una violazione degli artt. 3 e 8 CEDU, in relazione a un'ipotesi di violenza sessuale – non si è limitata a evidenziare in via generale il difetto di tempestività e completezza delle indagini, ma si è distinta per aver specificamente indicato come strada investigativa da privilegiare quella che avrebbe dovuto basarsi su attività di carattere scientifico e tecnologico, nella specie su analisi del DNA.[29]

L'insieme circoscritto, corrispondente alle tre pronunce citate, riesce a comporre un mosaico dal quale si ricavano, anzitutto, le remore della Corte e prendere posizioni nette in materia di uso della tecnologia nell'accertamento penale. In quest'ottica, emergono soprattutto le resistenze manifestate nella prima sentenza, cui fanno da contraltare spinte forti affidate alle opinioni separate. Non mancano di trasparire i pericoli di una discriminazione, spesso sottotraccia e poco riconoscibile, che potrebbero persino accentuarsi dinanzi all'uso di dati probatori biometrici. Mentre, il *caso Y c. Bulgaria* riflette la piena consapevolezza del giudice sovranazionale rispetto alla pregnanza delle strategie investigative basate sull'utilizzo di strumenti più moderni. La Corte ne fa significativamente oggetto delle obbligazioni positive procedurali che, sempre più spesso, vengono da essa riconosciute per sollecitare prassi nazionali capaci di assicurare l'avvio di indagini pronte ed effettive a tutela dei diritti umani.

4.2. L'attenzione crescente per il tema del riconoscimento facciale

Considerando il secondo tra i due gruppi di pronunce della Corte europea sopra individuati – il quale da più vicino interessa i temi del riconoscimento facciale – può essere citato anzitutto il caso *Gaughran c. UK*.[30] Il ricorrente – che era stato condannato per fatti criminosi considerati di non eleva-

29 Corte EDU, 20 febbraio 2020, *Y c. Bulgaria*.

30 Corte EDU, 13 febbraio 2020, *Gaughran c. Regno Unito*.

ta gravità, nell'Irlanda del Nord – lamentava il sequestro e la conservazione a tempo indeterminato, da parte delle forze dell'ordine, del corredo probatorio comprensivo di foto, impronte digitali e dati biologici.

Facendo riferimento all'art. 8 CEDU, la Corte di Strasburgo ha riconosciuto che la conservazione del profilo DNA e degli altri elementi in questione abbia costituito un'ingerenza nella vita privata del ricorrente. Parimenti, al centro della condanna della Corte EDU è stata posta anche la conservazione dell'immagine che ritraeva il ricorrente al momento del suo arresto, custodita a tempo indeterminato in un *database* locale che, in uso delle forze dell'ordine, si è avvalso anche di quel ritratto per applicare tecniche di mappatura e riconoscimento facciale.

La Corte EDU si è soffermata nel differenziare le funzioni dell'originaria acquisizione e della successiva conservazione dei dati, sottolineando che se la prima serve a individuare una determinata persona e collegarla alla commissione di uno specifico fatto criminoso, di cui è sospettata, la seconda persegue scopi più ampi. Mira, infatti, a contribuire all'identificazione di chi possa commettere reati in futuro, perseguendo la legittima finalità di prevenzione di atti criminosi. Ciò posto, vero è che agli Stati spetta un margine di discrezionalità, nel regolamentare la conservazione dei dati, tenendo conto di diversi fattori, tra cui la gravità del reato già addebitato, la necessità di effettuare detta conservazione e il rispetto delle garanzie individuali. Tuttavia, se un ordinamento nazionale oltrepassa tale margine – attestandosi sulla massima espansione del potere di avvalersi della conservazione di dati, persino senza limiti di tempo – possono prospettarsi vizi riguardo alla tutela dei diritti umani e la sua effettività.

Il Governo del Regno Unito, convenuto, faceva leva sull'asserita diretta proporzionalità tra la quantità dei dati custoditi e il numero di reati da prevenire, ritenuto crescente in base a ricerche statistiche incentrate sulle ipotesi di recidiva. Argomento, questo, disatteso dalla Corte europea nell'osservare come una sua aprioristica considerazione giustificherebbe una conservazione di elementi estesa e indiscriminata. L'interesse pubblico diretto ad arginare il novero dei casi 'irrisolti', ad avviso della Corte, deve infatti essere contemperato

con la tutela dei diritti fondamentali delle persone coinvolte e, in quest'ottica, il protrarsi illimitato della conservazione di dati avrebbe imposto un bilanciamento con le garanzie delle persone interessate e in precedenza condannate. Mentre, né, da un canto, raccolta e custodia dei dati erano state precedute da un vaglio adeguato, né – al di là di un potere spettante in casi eccezionali alle forze dell'ordine – ai diretti interessati spettava uno strumento per richiedere la cancellazione dei dati stessi in ragione di specifiche circostanze (come gravità e natura dei reati, età dei soggetti coinvolti, tempo trascorso, o esiti rieducativi raggiunti). Pertanto, è il sommarsi tra il carattere indiscriminato dei poteri di conservazione, da un lato, e la non azionabilità dei diritti compromessi a determinare un ingiustificato squilibrio tra interessi pubblici e garanzie individuali, in favore dei primi, con la conseguenza di un riscontrato superamento dei margini di discrezionalità fruibili dagli Stati, tramite forme di ingerenza nella vita privata sproporzionate e non necessarie.

Un caso ulteriore non è stato oggetto del riconoscimento di una violazione convenzionale da parte della Corte EDU, ma è meritevole di essere ricordato soprattutto per le importanti puntualizzazioni espresse in seno all'opinione concorrente di un giudice della Corte stessa. All'origine del caso *Beghal c. Regno Unito*[31] si poneva il pregiudizio lamentato dalla ricorrente che, cittadina francese residente nel Regno unito, era di ritorno verso quest'ultimo dopo aver fatto visita al marito detenuto in Francia. Fermata e condotta in una sala dell'aeroporto in seguito all'atterraggio, la signora – accompagnata da tre figli – veniva sottoposta a verifiche dirette a rivelare operazioni prodromiche ad atti terroristici.

Il principale riferimento normativo domestico risiede nell'allegato n. 7 del *Terrorism Act 2000* ('TACT'), che autorizza forze dell'ordine e funzionari doganali o impegnati nel controllo dei flussi migratori a fermare, interrogare e perquisire passeggeri all'interno di porti, aeroporti e terminal ferroviari internazionali. Svincolata da autorizzazioni preventive e da sospetti di coinvolgimento in attività terroristiche, l'attività è finalizzata proprio a prevenire queste ultime.

31 Corte EDU, 14 gennaio 2016, *Beghal c. Regno Unito*.

La persona da sottoporre all'accertamento, che può essere trattenuta per un lasso di tempo esteso sino a nove ore, è tenuta a fornire dietro richiesta dell'operatore "tutte le informazioni in suo possesso" e a non ostacolare lo svolgimento di alcun atto investigativo. Penalmente perseguibile, la mancata cooperazione è punita con la reclusione fino a tre mesi o con sanzione pecuniaria. Ciò posto, in applicazione dell'allegato cit., l'interessato, da un canto, ha il diritto di farsi assistere da una persona nominata e consultare un avvocato, dall'altro, ha l'obbligo di rendere disponibili impronte digitali e campioni biologici.

La pronuncia – pur riecheggiando quanto affermato in altri casi – presenta tratti distintivi legati proprio alla base normativa di riferimento. Infatti, sino a quel momento erano state prese in considerazione, per un verso, fonti che non mancavano di offrire strumenti di tutela dinanzi a ingerenze arbitrarie da parte dell'autorità procedente e, per altro verso, ipotesi di verifiche estranee al controllo dei porti e delle frontiere, in discussione nel caso in esame. Non potendo mutuare soluzioni più rigorose in precedenza raggiunte, la Corte europea – meno severa rispetto alle altre occasioni – ha valorizzato la circostanza che il Regno Unito, in quanto 'nazione insulare', concentri fisiologicamente i controlli nel contesto delle sue frontiere nazionali, per giustificare ampi margini di discrezionalità nell'effettuarli. Svincolandosi da argomentazioni precedenti e più incisive, ha ritenuto i poteri di cui all'allegato in questione sufficientemente circoscritti, escludendo vizi convenzionali.

Più precisamente, le argomentazioni della Corte di Strasburgo si sono articolate su più livelli. Se, in primo luogo, si è escluso un contrasto con l'art. 8 CEDU, per l'attestarsi delle intrusioni al di sotto di uno standard minimo, in secondo luogo – negando che pronunce precedenti potessero valere come riferimento utile – si è sottolineata l'importanza e la necessità dei controlli portuali e di frontiera. Controlli, peraltro, destinati a una limitata cerchia di persone, in viaggio da precise aree geografiche; nonché oggetto di prassi restrittive, di impatto ridotto ed estranee rischi di usi eccessivi, impropri e arbitrari. Tutto ciò, evidenziando la stretta finalizzazione dei controlli in discorso al monitoraggio di porti e frontiere e non, invece,

all'avvio di un'indagine penale: il che, secondo la Corte europea, giustificherebbe il loro uso svincolato da un 'ragionevole sospetto'. In chiusura, la Corte si è soffermata, peraltro, sul rilievo dello scopo sotteso a queste attività, volte alla prevenzione di atti terroristici. Ad avvalorare l'esclusione di violazioni dell'art. 8 CEDU e di una potenziale vulnerabilità dei viaggiatori per ingerenze arbitrarie dell'autorità, si è rimarcato il fondamento dei poteri esercitati dalle forze dell'ordine, supportati da una base legale che ne definisce i necessari limiti.

Non può sfuggire, però, l'importanza e la puntualità dell'opinione separata e dissenziente di un giudice,[32] il quale, nel paragonare la vicenda a casi esaminati in precedenza dalla Corte con maggior rigore, ha osservato come verifiche che impongano ai viaggiatori di rispondere a domande sui propri movimenti e attività, dietro la minaccia di sanzioni penali, risultano assai più invasive di un semplice controllo sull'identità e sul diritto all'ingresso nel Paese. Inoltre, ha obiettato come la prassi sino ad allora emersa, espressiva di una certa "moderazione" da parte delle autorità, non sia in grado di bilanciare *deficit* di determinatezza della fonte normativa. Dando risalto alla portata potenziale del potere (e non al suo utilizzo effettivo), il giudice ha espresso timori rispetto a esercizi arbitrari delle verifiche, in assenza di strumenti e doglianze per rilevare e contenere eventuali abusi. Soprattutto, ha paventato la possibilità, non monitorabile, che i controlli fossero attivati secondo discriminazioni a seconda di origine etnica o religione.

Ancora, sembra opportuno rammentare brevemente la vicenda relativa al caso *Peck c. Regno Unito*, ormai non più recente.[33] Il suo protagonista, soffrendo di depressione, mosso dal proposito del suicidio percorreva una strada trafficata armato di un coltello da cucina. Procuratesi delle ferite ai polsi si affacciava da un parapetto, ignaro della presenza di telecamere che riprendevano i suoi movimenti. Informate dai passanti, le forze dell'ordine sono intervenute facendo sì che all'uomo fosse assicurata la necessaria assistenza medica e, dopo rapidi accertamenti, lo hanno rilasciato accompagnandolo alla sua abitazione senza contestargli alcuna accusa.

32 Si tratta del giudice Kerr.

33 Corte EDU, 28 gennaio 2003, *Peck c. Regno Unito*.

Successivamente, venuto casualmente a sapere dell'esistenza di un filmato in cui si distingueva la sua immagine – divulgato anche nel corso di programmi televisivi – l'interessato ha cercato inutilmente di far valere i propri diritti in sede nazionale e, in seguito, si è rivolto alla Corte EDU, che non ha mancato di riscontrare la violazione degli artt. 8 e 13 CEDU.

Le pronunce selezionate e citate mostrano come lo strumento del riconoscimento facciale incida su una sfera di tutela che risulta oramai fortemente esposta a rischio. In una sfida sul campo dei diritti umani, v'è da notare come la giurisprudenza della Corte europea sia chiamata a giocare un ruolo centrale, anche (e qualche volta soprattutto) attraverso le opinioni separate espresse dai suoi giudici.

4.3. Il caso *Glukhin* c. Russia

Al di là dei due gruppi di casi sopra indicati, ve n'è uno che – più recente – merita una considerazione autonoma per la sua centralità rispetto all'argomento in esame, oltre che per il risalto avuto anche grazie al *web* e ai mass media. Il caso *Glukhin c. Russia*[34] riguardava la condanna di un uomo, in seguito a un procedimento di carattere amministrativo, per aver mancato di comunicare alle autorità la propria intenzione di svolgere una manifestazione di natura pacifica e individuale, a Mosca. Esibendo uno slogan provocatorio in difesa di un noto contestatore già arrestato, egli esibiva l'immagine di quest'ultimo, riprodotta in una sagoma creata *ad hoc*, in modo da nascondere le proprie sembianze.

Ebbene, la Corte europea ha ritenuto di affermare la violazione dei diritti umani dovuta all'uso, da parte delle forze dell'ordine, di procedure di riconoscimento facciale per reperire i dati personali del Sig. Glukhin. Più precisamente, questi è stato identificato e i suoi spostamenti sono stati tracciati tramite l'uso ad ampio raggio di videocamere a circuito chiuso, collocate in numerosi punti della città, inclusa la metropolitana e gli spazi ad essa dedicati.

34 Corte EDU, 4 luglio 2023, *Glukhin c. Russia*.

All'unanimità, la Corte EDU ha riscontrato violazioni da parte dello Stato russo sia dell'art. 8 che dell'art. 10 CEDU, com'è noto inerenti l'uno alla tutela della vita privata e familiare, l'altro alla libertà di espressione. L'elaborazione dei dati del ricorrente, infatti, è stata ritenuta spiccatamente intrusiva e incompatibile con i valori di una società democratica.

Con ciò, Il giudice europeo ha colto l'occasione per sottolineare come l'utilizzo delle procedure di riconoscimento facciale debba risultare necessario e proporzionato alla gravità dei fatti da perseguire. Requisiti che, nel contesto del caso in discorso, non sarebbero stati valutati dalle autorità domestiche. In più, a monte, la Corte ha evidenziato la mancanza di regole e forme di tutela nel sistema russo, in relazione all'impiego delle tecnologie usate, ponendo in luce l'esigenza di una disciplina completa e dettagliata. Al centro della pronuncia è stata posta, altresì, la carenza di una motivazione rispetto alla limitazione della libertà personale e alla condanna del ricorrente. In favore di quest'ultimo, alla luce dei vizi riscontrati, la Corte europea ha disposto oneri compensativi a carico dello Stato russo per i pregiudizi non patrimoniali sofferti e le spese legali sopportate.

La pronuncia, in realtà, non chiude del tutto gli interrogativi sull'utilizzo, legittimo o meno, della tecnologia in questione, secondo un approccio che si giustifica anche a fronte dell'esclusione della Federazione Russia dal Consiglio d'Europa, decisa il 16 marzo 2022, dopo una riunione straordinaria del Comitato dei Ministri, nel quadro della procedura di cessazione dello stato di membro del Consiglio stesso avviata in virtù dell'art. 8 dello Statuto di quest'ultimo. La Corte europea plausibilmente – pur potendo stabilire chiari limiti all'uso delle videocamere in luoghi pubblici – nella consapevolezza che la pronuncia non avrebbe trovato esecuzione nel Paese interessato, ha preferito evitare prese di posizioni nette, capaci di pesare nell'orizzonte di altri Stati. La sentenza, tuttavia, rappresenta un importante punto di riferimento per affrontare le principali problematiche inerenti all'ambito in esame, anche nella formulazione di una fonte[35] dell'Unione europea dedicata all'argomento.

35 Regolamento *Artificial Inteligence Act* – AIA.

La sentenza è intervenuta, infatti, in un momento in cui il dibattito al riguardo era particolarmente intenso. E la risposta temperata della Corte europea può avere inciso sulla discussione oscillante tra le opzioni che consideravano un radicale divieto come l'unica soluzione compatibile con le garanzie individuali e quelle, meno rigorose, che puntavano su una regolamentazione del riconoscimento facciale.[36] In linea di massima, il provvedimento pesa in favore della seconda tendenza, fatta propria dalla Commissione e dal Consiglio, volta all'introduzione di una disciplina esaustiva. Tuttavia, la Corte europea non si è spinta sino a fornire indicazioni rispetto alla tutela dei diritti umani o capaci di incidere più esplicitamente sul futuro delle fonti UE.

Un punto particolarmente importante può rischiare di passare in secondo piano. Concerne l'ambito dell'onere probatorio e, pertanto, si proietta sul piano relativo alla presunzione di innocenza. Il profilo può essere sintetizzato ricordando che, secondo il ricorrente, la polizia avrebbe utilizzato strumenti di riconoscimento facciale per identificarlo e localizzarlo, tuttavia egli non è stato in grado di dimostrare questo aspetto.

In questo quadro, la Corte europea ha mostrato il convincimento che quanto riportato dal ricorrente fosse 'plausibile' e che un siffatto uso dei dati biometrici avrebbe causato ina interferenza nella sua vita privata.

Più precisamente, il riconoscimento facciale sarebbe stato usato *ex post* sia per identificare l'uomo, sia per localizzare la sua posizione e, dunque, per arrestarlo. In quest'ottica, seppure si fonda su una base legale, la realizzata interferenza nella sfera individuale non corrisponde agli *standard* richiesti dalla legge. E ciò assume rilievo nel contesto di una consolidata posizione della Corte europea che mira a circoscrivere l'incidenza sui diritti umani, quantomeno entro i limiti della sua prevedibilità e trasparenza. Ossia, nella misura in cui all'accusato deve essere consentito conoscere agevolmente le conseguenze della violazione e prevederle. Mentre, la normativa in materia, nell'ordinamento russo, è formulata in maniera ampia, senza che siano indicati i presupposti per l'uso della tecnologia, né siano previste un'autorizzazione o pro-

36 Neroni Rezende 2023.

cedure per esaminare utilizzare e conservare i dati ottenuti, o predisposti meccanismi di controllo e rimedi. In questo caso, peraltro, il riconoscimento facciale era stato utilizzato per fini di prevenzione di attività criminosa.

L'uso è stato ritenuto dalla Corte sproporzionato, in considerazione sia della natura pacifica della protesta, che non ha creato alcun pericolo per la collettività o per la sicurezza dei trasporti, nonché della fattispecie contestata al ricorrente dalle autorità russe, di scarsa gravità. In definitiva, non occorreva fare ricorso a questa tecnologia e il suo utilizzo è stato considerato non necessario in una società democratica. Ragione per cui la Corte EDU ha riscontrato le violazioni soprindicate, relative agli artt. 8 e 10 CEDU.

La decisione è coerente con la tendenza a un approccio della Corte EDU improntato al *self-restraint*, che essa solitamente segue in tema di sorveglianza. Di tale approccio, ambiguo e aperto a letture contrapposte può essere un esempio la sentenza della Grande Camera sul caso *Big Brother Watch c. Regno Unito*,[37] capace di essere considerata talvolta come un invito all'osservanza delle garanzie individuali, talaltra come un'apertura verso una sorta di 'normalizzazione' della sorveglianza di massa.[38]

5. Brevi considerazioni conclusive

Si ricava, in definitiva, una capacità della giurisprudenza della Corte europea e, in particolare, della sentenza sul 'caso Glukhin' di mettere in evidenza le principali questioni e l'esigenza di chiarezza della disciplina normativa. I sistemi di riconoscimento facciale, infatti, producono implicazioni significative nel contesto dei valori fondamentali della società democratica e, perciò, non possono essere affidati a un'ampia discrezionalità dell'interprete.

37 Corte EDU, Grande Camera, 25 maggio 2021, *Big Brother Watch e altri c. Regno Unito*, che ha condannato il Governo del Regno Unito per aver autorizzato misure di sorveglianza massiva delle telecomunicazioni in violazione della CEDU.

38 Milanovic 2021.

La Corte EDU, tuttavia, non ha riscontrato un'astratta incompatibilità tra riconoscimento facciale e tutela dei diritti umani, aggirando la questione e attenendosi al suo ruolo legato alle peculiarità del caso, con rigore ancor più stretto che in altre occasioni. Non ha neppure operato distinzioni tra sistemi di riconoscimento facciale *ex post* e *live*, di impatto diverso sulla tutela della vita privata, fermandosi a un livello di analisi superficiale. Ne deriva che l'affermata presenza di una violazione dell'art. 8 CEDU non riesce a escludere e a delimitare ambiti di applicazione dell'istituto di cui sopravviva la *fairness*. Gli *standard* di '*quality of the law*' che emergono – qualche volta timidamente – dalla giurisprudenza della Corte EDU, di fronte allo strumento in esame rappresentano perciò tuttora un obiettivo da studiare e raggiungere.

V'è da chiedersi come l'evoluzione della giurisprudenza della Corte EDU possa aver inciso sullo sviluppo del dibattito e delle fonti dell'Unione europea. Per molti aspetti, l'assetto della giurisprudenza della Corte EDU è più rilevante per ciò che non viene specificato che per ciò su cui manifestamente essa si esprime. E non può sfuggire come molte indicazioni significative siano rintracciabili nel contesto delle opinioni separate che, in questa materia, esercitano un ruolo di 'sentinella' di problematiche di rilievo, in maniera ancor maggiore di quanto già accada di consueto.[39]

In particolare, la pronuncia relativa al 'caso Glukhin' implicitamente esclude che dai principi fissati dalla CEDU si ricavi la necessità di una integrale esclusione della tecnologia in questione. Quantomeno, la Corte EDU ha evitato di influire eccessivamente sulla discussione inerente al quadro normativo in evoluzione, nella consapevolezza del considerevole impatto che la giurisprudenza della Corte di Strasburgo finisce per avere sul sistema delle fonti dell'Unione europea, anche alla luce dell'art. 6, par. 3, TUE.

Dal canto loro, se le fonti dell'UE sembrano adesso assestarsi attorno a un divieto del riconoscimento facciale *live* e ad aperture rispetto a quello *ex post*, occorre ancora fissare in maniera più stabile la sagoma delle attività che possano ritenersi da ammettere. Anche rispetto alla seconda modalità, d'altra parte, rilevano alcune preoccupazioni, relative ad

39 Pinto de Albuquerque-Cardamone 2019.

esempio alla raccolta degli elementi da immagazzinare in banche dati, tratti da fonti accessibili sul *web*, o da altre risorse non specificate. Nessuno sbarramento sinora è stabilito rispetto ad attività di *social media scraping* ed *emotion recognition*. Mentre, ad esempio, si potrebbe persino prospettare la creazione di sistemi capaci di 'catalogare' persone che tengano in pubblico comportamenti semplicemente sospetti, in dispregio alle loro garanzie.

Ad ogni modo, anche altri punti critici, sinora trascurati, necessitano di riflessioni. L'entusiasmo per la fruibilità dello strumento ha lasciato in secondo piano aspetti procedurali di grande rilievo. Nel dibattito sulle nuove norme dell'Unione europea, è prevalsa l'idea invero non del tutto appagante di un'autorizzazione da parte di un giudice o di un'autorità indipendente, senza che si traccino regole precise sulla richiesta e la sua valutazione, nonché su una supervisione del *placet*. Tra gli altri passaggi delicati, nell'utilizzo del riconoscimento facciale nel contesto del procedimento penale, spicca poi quello inerente al ruolo della difesa tecnica. Priva di un'effettiva incidenza, essa è destinata a un coinvolgimento solo successivo, a fronte di risultati investigativi già raggiunti e spesso tra l'altro anche divulgati.

Inoltre, se i vantaggi dell'uso della tecnologia in esame emergono con chiarezza, per varie finalità, occorre prendere atto dell'intera gamma dei rischi, in termini di 'falsi' positivi e negativi, o di possibili usi e abusi dei sistemi, non del tutto controllabili né prospettabili anticipatamente. Il che suscita timori anche nell'ottica di errori giudiziari, o di ingerenze nella sfera dei diritti individuali di un numero illimitato di persone. Come osservato dal Direttore esecutivo del *Surveillance Technology Oversight Project* di New York, Albert Fox Cahn, in relazione agli impieghi di questo mezzo nei contesti di episodi bellici, esso presenta un margine di fallacia notevole e può definirsi "una tecnologia benintenzionata" capace di "ritorcersi contro e danneggiare proprio quelle persone che dovrebbe invece aiutare". E ciò considerato che, "nel momento in cui si introducono questi sistemi e i relativi *database*", "non si ha più il controllo su come verranno usati e abusati".[40]

40 Per la citazione, Darretta 2022.

Bibliografia

Borgia 2021: Borgia G., *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in Legislazione penale, 2021, 1-23.

Colacurci 2022: Colacurci M., *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in Sistema penale, 12 settembre 2022.

Currao 2021: Currao E., *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in Diritto penale e uomo, 5/2021, 1-25.

Dalia-Ferraioli 2016: Dalia A.A., Ferraioli M., *Manuale di diritto processuale penale*, Milano, 2016, p. 352.

Darretta 2022: Darretta S., *Riconoscimento facciale: Clearview AI "entra in guerra" contro la Russia*, in www.datamagazine.it, 23 marzo 2022.

Della Torre 2020: Della Torre J., *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in Diritto penale contemporaneo-Rivista trimestrale, 1/2020, 231-247.

De Simone 2023: De Simone F., *Una nuova tipologia di misure di prevenzione: algoritmi, intelligenza artificiale e riconoscimento facciale*, in Archivio penale, 2/2023, 1-36.

Lopez 2019: Lopez R., *La rappresentazione facciale tramite software*, in *Le indagini atipiche*, a cura di Scalfati A., Torino, 2019, 239-257.

Lopez 2022: Lopez R., *Videosorveglianza biometrica tramite riconoscimento facciale*, in Processo penale e giustizia, 3/2022, 798-803.

Marcolini 2010: Marcolini S., *Le cosiddette perquisizioni* '*on line*' (*o perquisizioni elettroniche*), in Cassazione penale, 7-8/2010, 2855-2868.

Marcolini 2015: Marcolini S., *Le indagini atipiche a contenuto tecnologico nel processo penale*, in Cassazione penale, 2/2015, 760-792.

Mastro 2022: Mastro D., *Le cause degli errori giudiziari e i meccanismi di prevenzione e riparazione delle condanne e imputazioni ingiuste*, in Revista Brasileira de Direito Processual Penal, 2022, 1371-1415.

Milanovic 2021: Milanovic M., *The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments*, in Big Brother Watch and Centrum för rättvisa, in www.ejiltalk.org, 26 maggio 2021.

Neroni Rezende 2020: Neroni Rezende I., *Facial Recognition for Preventive Purposes: The Human Rights Implications of Detecting Emotions in Public Spaces*, in *Investigating and Preventing Crime in the Digital Era*, a cura di Bachmaier L., Winter S., Springer, 2020, 67 ss.

Neroni Rezende 2020: Neroni Rezende I., *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective*, in Sage Journals, 13 agosto 2020.

Neroni Rezende 2023: Neroni Rezende I., *Glukhin and the EU regulation of facial recognition: Lessons to be learned?*, in https://europeanlawblog.eu, 19 settembre 2023.

Parlato 2020: Parlato L., *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, in Processo penale e giustizia, 2/2020, 291-307.

Pinto de Albuquerque-Cardamone 2019: Pinto de Albuquerque P., Cardamone D., *Efficacia della dissenting opinion*, in Questione giustizia, 2019, Gli speciali, La Corte di Strasburgo, 148-155.

Quattrocolo 2020: Quattrocolo S., *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, Springer, 2020.

Sacchetto 2019: Sacchetto E., *Spunti per una riflessione sul rapporto tra biometria e processo penale*, in Diritto penale contemporaneo-Rivista trimestrale, 2/2019, 465-480.

Sacchetto 2020: Sacchetto E., *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in Legislazione penale, 2020, 1-14.

Scalfati 2011: Scalfati A., *La deriva scientista dell'accertamento penale*, in Processo penale e giustizia, 5/2011, 144-150.

Scalfati 2014: Scalfati A., *Premessa*, in *Le indagini atipiche*, a cura di Scalfati A., Torino 2014, XV-XVIII.