

**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

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

Director

Mario Varvaro

Scientific Board

Christian Baldus (Heidelberg)
Licia Califano (Urbino)
Luigi Capogrossi Colognesi (Roma)
Marta Cartabia (Milano)
Sara Domianello (Messina)
Iole Fagnoli (Bern & Milano)
Luigi Ferrajoli (Roma)
Giovanni Fiandaca (Palermo)
Enrico Follieri (Foggia)
Flavia Frisone (Lecce)
Elisabetta Grande (Alessandria)
Patrizia Guarnieri (Firenze)
Soazick Kerneis (Paris)
Umberto Laffi (Pisa)
Rita Lizzi (Perugia)
Paola Maggio (Palermo)
Laura Moscati (Roma)
Luca Nogler (Trento)
Annick Peters-Custot (Nantes)
Emanuela Prinzivalli (Roma)
Serena Quattrocchio (Alessandria)
Eugenio Ripepe (Pisa)
Boudewijn Sirks (Oxford)
Giusto Traina (Paris & Lecce)
Cristina Vano (Napoli)
Giovanna Visintini (Genova)
Andreas Wacke (Köln)

Editorial Board

Laura Calandriello
Rosaria Crupi
Monica De Simone
Manfredi Matassa
Veronica Virga

E-mail: hllh@unipa.it

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

© Copyright 2024 New Digital Frontiers srl
Via Serradifalco, 78
90145 Palermo - Italia
www.newdigitalfrontiers.com

INDICE GENERALE

NOTA DELLE CURATRICI

VII

PARTI I. LA PROVA DEL DNA NEL PROCESSO PENALE

1

PASQUALE ALONGI

INTRODUZIONE: 120 ANNI DI POLIZIA SCIENTIFICA

3

PAOLA DI SIMONE

ACCERTAMENTI GENETICO-FORENSI A FINI
IDENTIFICATIVI NELLE INDAGINI DI POLIZIA
GIUDIZIARIA. LA BANCA DATI NAZIONALE DEL DNA

11

LUISA BETTIOL

LA PROVA DEL DNA NEL PROCEDIMENTO PENALE

27

PARTI II. DALLE IMPRONTE DIGITALI AL RICONOSCIMENTO FACCIALE

45

MASSIMO TAORMINA

LE IMPRONTE DIGITALI QUALE METODO
IDENTIFICATIVO DALLE ORIGINI AD OGGI

47

GIOVANNI TESSITORE

RICONOSCIMENTO AUTOMATICO DEL VOLTO
E CONFRONTO IN AMBITO FORENSE

61

ANNALISA MANGIARACINA

IL RICONOSCIMENTO FACCIALE: NUOVE SFIDE
NEL PROCESSO PENALE

77

LUCIA PARLATO

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

95

PIERANGELO PADOVA

RICONOSCIMENTO AUTOMATICO DEL VOLTO
TRA ESIGENZE INVESTIGATIVE E TUTELA
DELLA PRIVACY

121

MASSIMO MOTISI

LUCI E OMBRE DELLA PROVA SCIENTIFICA
NEL PROCESSO PENALE

133

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

IL RICONOSCIMENTO FACCIALE: NUOVE SFIDE NEL PROCESSO PENALE

ANNALISA MANGIARACINA

Università degli Studi di Palermo

Abstract: AI and especially facial recognition techniques are increasing their use also with the aim of prosecuting criminal offences. In Italy, the Data Protection Authority has prohibited the use of facial recognition in real time mode. At national level, it should be necessary a clear regulation of these instruments that have a consistent impact on fundamental rights of individuals.

Parole chiave: Corte di Strasburgo; riconoscimento facciale; Garante per la privacy.

1. Lo scandalo 'Clearview'

Il corpo umano è "una miniera a cielo aperto dalla quale attingere dati ininterrottamente".¹ Nel contesto delle tecniche biometriche e, più nello specifico, del riconoscimento facciale, la miniera è rappresentata dal volto di ciascun individuo, dotato di specifiche caratteristiche. Il riconoscimento facciale² consente, infatti, l'identificazione automatica di un soggetto mediante il confronto tra la fotografia o il video che ne

1 In questi termini Rodotà 2003: 10: «Lo ripetiamo: il corpo in sé sta diventando una password. La fisicità prende il posto delle astratte parole chiave, sostituite da impronte digitali, geometria della mano o delle dita o dell'orecchio, iride, retina, tratti del volto, odori, voce, firma, uso di una tastiera, andatura, Dna».

2 In argomento v. l'ampio lavoro di Mobilio 2021. Secondo il *Parere 2/2012 relativo al riconoscimento facciale nell'ambito dei servizi online e mobili*, adottato dal *Working Party 29*, in data 22 marzo 2012, il riconoscimento facciale può essere definito come un trattamento automatico di immagini digitali che contengono i volti di persone ai fini di identificazione, autenticazione, verifica o categorizzazione di tali persone e consta di un processo distinto nelle seguenti fasi: acquisizione dell'immagine, ossia il processo di rilevamento dei tratti del volto di una persona e la conversione in formato digitale; individuazione della presenza di un volto all'interno di un'immagine digitale; attenuazione delle variazioni all'interno delle regioni del volto individuate (si pensi alla conversione in una dimensione *standard* o all'allineamento delle distribuzioni del colore); estrazione di caratteristiche dell'immagine digitale di una persona; registrazione dell'immagine e / o del modello di riferimento per un successivo confronto; misurazione delle somiglianze tra una serie di caratteristiche del modello con quelle già registrate nel sistema.

raffigurano il volto e le immagini contenute in un database. Un'attività non certamente 'neutra'. I dati biometrici, secondo la definizione contenuta nell'art. 3 della Direttiva 2016/680/UE,³ sono i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; peraltro, in quanto riconducibili alla categoria dei dati sensibili, ex art. 10 della medesima Direttiva, necessitano di garanzie rafforzate.

Nelle precedenti relazioni si è discusso dell'estrazione del profilo del DNA, del rilevamento delle impronte digitali, tutti istituti comunemente utilizzati nello svolgimento delle attività d'indagine, con grande successo. Ebbene, il riconoscimento facciale, a differenza delle altre metodiche di identificazione biometrica basate sulle caratteristiche fisiologiche di un individuo,⁴ ha un vantaggio evidente: quello di non essere, almeno all'apparenza, uno strumento invasivo, non determinando alcuna forma di coazione fisica diretta sulle persone, potendosi prescindere dalla collaborazione del soggetto destinatario. Peraltro, il volto è difficile da nascondere – salvo che il soggetto non lo copra con una mascherina⁵ – facile da osservare e da 'acquisire' sia nello spazio fisico (ad esempio, mediante le videocamere di sorveglianza installate soprattutto negli spazi pubblici) sia in quello digitale (pensiamo alle immagini caricate sui diversi social network come Facebook, Instagram ...).

Tuttavia, le tecniche di riconoscimento facciale presentano rischi molto elevati "sia per la notevole probabilità di sviluppo di risultati non attendibili, e dunque, di identificazioni errate, sia per la strumentalizzazione a fini discriminatori e

3 Si tratta della Direttiva relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

4 Sulle diverse tecniche di identificazione biometrica v. Sacchetto 2019: 469 ss.

5 È quanto avvenuto a Hong Kong in occasione di alcune manifestazioni di protesta. <https://www.linkiesta.it/2019/10/giovani-proteste-hong-kong-riconoscimento-facciale/>.

di controllo politico e sociale", come dimostra l'esperienza di paesi come la Cina.⁶

Il tema ha assunto rilievo dirompente, anche in Europa, a seguito della nota 'vicenda Clearview', così denominata in ragione della società statunitense – 'Clearview' appunto – che aveva creato un motore di ricerca per il riconoscimento facciale (*facial recognition search engine*). Questa piattaforma offriva alle autorità pubbliche (forze dell'ordine) di diversi paesi, anche europei, un servizio di ricerca di immagini all'interno di un proprio database. Mediante tecniche di *web scraping* – normalmente vietate dai gestori dei siti, in particolare di social network – la società raccoglieva foto pubblicamente accessibili da siti (o video disponibili in rete), per poi elaborarle con tecniche biometriche. Una volta indicizzate, queste immagini potevano essere arricchite con i metadati disponibili associati (ad esempio, la pagina web da cui era stata presa, la data di nascita della persona ritratta, la nazionalità, la lingua parlata ecc.), cosicché quando il software identificava una corrispondenza, estraeva dal database tutte le relative immagini e le presentava al cliente del servizio come risultato della ricerca unitamente ai metadati e ai link associati, permettendo così di risalire a ogni singola pagina sorgente. L'immagine così raccolta rimaneva nel database anche nell'ipotesi in cui la foto originaria o la pagina web di riferimento fosse stata successivamente rimossa o resa privata. Dall'indagine condotta è risultato che anche le autorità italiane erano tra i 'beneficiari' di questi dati.⁷ Nel 2022, il Garante per la privacy⁸ è quindi intervenuto per sanzionare la condotta di Clearview, ritenendo che l'attività svolta non consistesse, diversamente da quanto dichiarato dalla società stessa, nella mera classificazione di individui sulla base di caratteristiche note, ma nella gestione di dati biometrici che consentiva un tracciamento nel tempo delle persone a essi associate. Come osservato,

6 Sacchetto 2020: 9 ss.

7 Report for the Greens/EFA in the European Parliament, *Biometric & behavioural mass surveillance in EU Member States*, ottobre 2021, p. 18.

8 GPD, Ordinanza di ingiunzione nei confronti di Clearview AI- 10 febbraio 2022.

le informazioni in questione formano oggetto di archiviazione nel database di Clearview e vengono arricchite nel tempo con altre estratte da nuovi *template* idonei a riflettere anche i cambiamenti fisici avuti dallo stesso soggetto, come emerge dall'esame di alcuni dei reclami proposti all'Autorità ... Ne discende che Clearview non offre come risultato della ricerca una semplice corrispondenza, ma anche un archivio di risorse che si snoda attraverso il tempo. La valutazione di tale circostanza, unitamente alla finalità comparativa sopra evidenziata, è idonea ad integrare, come richiesto nel Considerando 24, un'attività assimilabile al controllo del comportamento dell'interessato in quanto posta in essere tramite il tracciamento in internet e la successiva profilazione.

2. I software di riconoscimento facciale

Molteplici sono gli scopi per i quali i software di riconoscimento automatico facciale possono essere utilizzati: al di là delle comuni finalità commerciali, rilevano per lo più ai fini di identificazione, autenticazione / verifica o categorizzazione degli individui. La verifica e l'identificazione si occupano di identificare le caratteristiche peculiari dell'individuo per stabilirne l'identità personale. La categorizzazione è invece utilizzata per dedurre dalle immagini del volto informazioni sulle caratteristiche dell'individuo, come il sesso, l'età o l'etnia.

Identificazione e verifica riguardano la corrispondenza delle caratteristiche uniche degli individui (occhi, naso, bocca) per determinare la loro identità individuale; in ipotesi di verifica biometrica, il soggetto dichiara la propria identità e il sistema effettua un confronto 'uno a uno' (*one-to-one matching*) tra il modello biometrico rilevato e quello memorizzato e corrispondente all'identità dichiarata; viceversa, in quella di identificazione biometrica, il sistema effettua un confronto uno a molti, tra il modello rilevato e quelli disponibili contenuti in un database. La tecnologia restituisce un punteggio per ogni confronto, indicativo della 'probabilità' che le due immagini si riferiscano alla stessa persona. Accanto a stru-

menti concepiti per condurre l'analisi di volti rappresentati in immagini statiche, ve ne sono altri in grado di processare in diretta più flussi video provenienti sia da telecamere fisse, sia da dispositivi portatili mobili come *body cameras* o droni.

La modalità cd. *Real-Time* permette, dunque, di conoscere immediatamente se un determinato individuo sospettato di aver commesso o, addirittura, di poter commettere un reato, si trovi nel luogo sottoposto a osservazione. Chiaramente, in questo caso il sistema è in grado di immagazzinare informazioni relative ad "un numero indeterminato di soggetti ... spesso estranei all'attività di indagine".⁹ Quest'ultima modalità pone i maggiori profili di criticità in quanto comporta, in linea potenziale, una sorveglianza di massa, in assenza di qualunque forma di consenso da parte delle persone oggetto del trattamento e, soprattutto, di regolamentazione giuridica.

Occorre però evidenziare come i possibili impieghi delle tecniche di riconoscimento facciale non si esauriscano qui: queste possono essere utilizzate per classificare le emozioni facciali (come un sorriso) ovvero gli stati emotivi di una persona (felicità, tristezza, rabbia), e per stabilire se i soggetti stanno mentendo o dicendo la verità. Quest'ultima tecnica è stata utilizzata ai confini di alcuni Paesi europei (Grecia, Ungheria e Lettonia) nel contesto del progetto *Integrated Portable Control System (iBorderCtrl)*:¹⁰ si tratta di un 'sistema intelligente di rilevamento delle menzogne' che permette di tracciare il profilo dei viaggiatori sulla base di un'intervista computerizzata effettuata con la webcam del passeggero prima del viaggio e un'analisi basata sull'intelligenza artificiale di 38 microgesti. Viva preoccupazione è stata espressa dal Parlamento europeo per questi progetti, con invito alla Commissione, tramite strumenti legislativi e non legislativi e, ove necessario, mediante procedure d'infrazione, a introdurre il divieto di trattamento dei dati biometrici, comprese le immagini facciali, per finalità di applicazione della legge, tali da determinare una sorveglianza di massa negli spazi accessibili al pubblico.

9 Borgia 2021: 4 s.

10 Sul funzionamento di questo sistema e sulle problematiche v. De Simone 2023: 11 ss.

3. La situazione in Italia: gli interventi del Garante per la privacy

Nel nostro paese, il sistema automatico di riconoscimento delle immagini (acronimo SARI) è nella disponibilità, fin dal 2017, della Polizia di Stato e dei Carabinieri, su iniziativa del Ministero degli Interni che ha iniziato a sviluppare lo strumento con un'azienda privata.¹¹ Il parere reso dal Garante per la privacy il 25 luglio 2018,¹² rispetto al software denominato 'SARI-Enterprise' per la ricerca di volti "a partire da immagini statiche su banche dati di grandi dimensioni", ha legittimato il suo utilizzo, escludendo qualsiasi violazione della disciplina prevista dalla direttiva 2016/680/UE, così come attuata nel nostro ordinamento attraverso il d.lgs. 18 maggio 2018, n. 51. Ciò sul presupposto che non si sarebbe realizzato "un nuovo trattamento di dati personali", bensì "una nuova modalità di trattamento" dei dati biometrici. Si è infatti affermato che, se in precedenza le ricerche a fini identificativi nella banca dati A.F.I.S. (*Automated Fingerprint Identification System* – ovvero il Sistema automatizzato di identificazione delle impronte digitali), integrata dal Sottosistema anagrafico S.S.A. (contenente oltre le foto-segnalistiche dei pregiudicati, anche i dati anagrafici e le informazioni riguardanti le loro caratteristiche biometriche acquisite in sede di foto segnalamento), venivano condotte mediante l'inserimento manuale da parte dell'operatore dei connotati identificativi del soggetto da identificare o verificare, da quel momento in poi, siffatta operazione è avvenuta in modo automatico, attraverso l'immissione nel sistema dell'immagine fotografica. Il Garante per la privacy¹³ scrive quindi che

il trattamento in argomento costituisce un mero ausilio all'agire umano, avente lo scopo di velocizzare l'identificazione, da parte dell'operatore di polizia, di un soggetto ricercato della cui immagine facciale si disponga, ferma restando l'esigenza dell'intervento

11 Sul tema v. le riflessioni, tra i tanti, di Colacurci 2022: 37 ss; Lopez 2022: 798 ss.

12 GPD, Parere sul sistema "SARI-Enterprise", n. 440, 25 luglio 2018.

13 GPD, Sistema automatico di ricerca dell'identità di un volto, n. 440, 26 luglio 2018.

dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato.

Ebbene, le disposizioni che disciplinano la suddetta banca dati sono state considerate sufficienti a soddisfare quanto stabilito dall'art. 7 del d.lgs. n. 51/2018, secondo cui il trattamento dei "dati biometrici intesi a identificare in modo univoco una persona fisica", in quanto *species* del *genus* "dati particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali", deve essere "specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento".

Diversa è stata, invece, l'opinione espressa dallo stesso Garante per la privacy¹⁴ con riferimento al sistema denominato 'SARI Real-Time' e utilizzato "per il riconoscimento in tempo reale di volti presenti in flussi video provenienti da telecamere". In questo caso, 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 migliaia di immagini. 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, sia 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. 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 SARI, così da poter segnalare eventuali corrispondenze future, incrementando in tal modo la possibilità di prossimi *matches*. Se, invece, il tentativo si conclude positivamente, per entrambe le modalità applicative del programma, 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.

14 GPD, Parere sul sistema 'SARI Real-Time', n. 127, 25 marzo 2021.

Si tratta di uno strumento del tutto inedito, dal momento che “l'identificazione di una persona ... comporta il trattamento biometrico di tutte le persone che circolano nello spazio pubblico monitorato”. Pertanto, prosegue il Garante, “si determina una evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui”. Alla luce di questa premessa, nell'esaminare le diverse fonti normative indicate dal Ministero ai fini del rispetto, innanzitutto, del principio di legalità del trattamento ex art. 7 del d.lgs. n. 51/2018, il Garante ha chiarito in primo luogo che la base legale non può essere ravvisata nello stesso d.lgs. n. 51/2018. Quanto all'art. 1 del TuLPS, si sottolinea che tale disposizione stabilisce i compiti generali secondo cui si articola l'attività dell'Autorità di pubblica sicurezza e, pertanto, non può costituire una previsione che “autorizza specificamente” il trattamento in questione. Rispetto al d.P.R. 15 gennaio 2018, n. 15 relativo al trattamento dei dati attraverso sistemi di videosorveglianza e di ripresa fotografica, audio e video, se ne esclude la rilevanza in quanto “ontologicamente diversi da quelli” biometrici in esame. A supporto di tale affermazione viene richiamato il regolamento 2016/679/UE, a cui la direttiva 2016/680/UE – come noto – è legata da un rapporto di complementarità. Nello specifico, il cd. GDPR, al considerando n. 51, chiarisce che “le fotografie” non “rientrano” sempre e comunque “nella definizione di dati biometrici”, ma “soltanto quando s[ono] trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca ... di una persona fisica”.

Rilevato che il ‘SARI *Real-Time*’ risulta concepito non solo per ‘coadiuvare’ le “Forze di Polizia nella gestione dell'ordine e della sicurezza pubblica”, ma anche per rispondere “a specifiche esigenze di Polizia Giudiziaria”, il Garante si sofferma da ultimo sui molteplici articoli del codice di rito richiamati nella documentazione ministeriale (artt. 134 co. 4, 234, 266 e 431 co. 1 lett. b e artt. 55, 348, 354 e 370 c.p.p.), evidenziando come nessuno di essi preveda il trattamento di dati biometrici e, pertanto, non possono integrare “quella fonte normativa specifica richiesta dall'art. 7” del d.lgs. n. 51/2018. In definitiva, manca una “base giuridica idonea”, il che rende l'implemen-

tazione del ‘SARI *Real-Time*’ non conforme alla normativa eurounitaria in tema di trattamento dei dati personali per finalità di *law enforcement*.

Problematiche analoghe sono state affrontate nel Regno Unito, dove, nel 2019, la *High Court of Justice*¹⁵ ha adottato una pronuncia con la quale, per la prima volta a livello europeo, si è affrontata la questione della compatibilità con i diritti fondamentali dell'utilizzo, da parte della polizia, di mezzi di riconoscimento facciale. Nello specifico, la Corte si è occupata del sistema “AFR *Locate*” che prevede la ripresa *live* tramite telecamere dei volti dei soggetti che si trovino in determinati luoghi di interesse, finalizzata all'estrazione del profilo facciale di questi individui; le informazioni ottenute sono poi confrontate, tramite un software, con i modelli biometrici di persone inserite in una lista *ad hoc* più ristretta preparata dalla polizia per l'evento di interesse (cd. *watchlist*). Con i motivi, il ricorrente lamentava la lesione del diritto alla riservatezza, ex art. 8 § 2 Cedue; la violazione della normativa europea e nazionale in tema di protezione dei dati personali, nonché dell'*Equality ACT* del 2010, lamentando il rischio che il software di *facial recognition* fosse affetto da *bias* cognitivi nei confronti delle donne e di minoranze etniche. Tutte le censure sono state però rigettate.

Come auspicato, la decisione, tuttavia, è stata successivamente ribaltata dalla Corte di appello¹⁶ che, in linea di principio, ha affermato come l'uso di dispositivi di riconoscimento facciale per finalità di *law enforcement* possa considerarsi un'interferenza ragionevole rispetto al diritto al rispetto della vita personale, alla duplice condizione che sussista un'idonea base regolamentare e che il relativo uso sia strettamente proporzionale allo scopo da conseguire. Nel caso di AFR *Locate*, però, la Corte ha rilevato che i criteri e i limiti del relativo utilizzo non erano stati anticipatamente predeterminati dalla polizia, lasciando agli agenti spazi di discrezionalità eccessiva sia per quanto concerne i soggetti da inserire nella *watchlist* che per la scelta dei luoghi pubblici in cui collocare i disposi-

15 Bridges, *R (On Application of) v The Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) – 4 settembre 2019. Sulla pronuncia v. Della Torre 2020: 231 ss.

16 Court of Appeal, Civil Division, [2020] EWCA Civ 1058, Bridges.

tivi di riconoscimento facciale. In secondo luogo, la Corte ha giudicato il sistema illegittimo anche perché la polizia aveva omissso di svolgere una preventiva valutazione di impatto sulla protezione dei dati personali, come espressamente richiesto dal *Data Protection Act*, con conseguente mancata valutazione in ordine alla sussistenza di eventuali rischi per i diritti e le libertà degli interessati. Ulteriori profili di illegittimità sono stati rinvenuti nella mancata preventiva verifica di eventuali *bias* di natura razziale o sessuale nell'algoritmo, in violazione del divieto di discriminazione posto a carico delle pubbliche autorità. In conclusione, si formulava l'auspicio che trattandosi di "a novel and controversial technology", tutte le forze di polizia che intendano utilizzarlo in futuro "wish to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias".

4. L'intervento poco chiaro del legislatore italiano

Tornando alla situazione italiana, è da rilevare che, dopo la decisione del Garante per la privacy, in sede di conversione in legge,¹⁷ con modificazioni, del d.l. 8 ottobre 2021, n. 139 (cd. decreto capienze), recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali, si è posta una moratoria sull'uso di sistemi di sorveglianza con tecniche di riconoscimento facciale. L'art. 1, comma 9, del menzionato d.l. n. 139/2021, stabilisce che in considerazione di quanto disposto dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, nonché dalla Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dell'esigenza di disciplinare conformemente i requisiti di ammissibilità, le condizioni e le garanzie relativi all'impiego di sistemi di riconoscimento facciale, nel rispetto del principio di proporzionalità previsto dall'art. 52 della Carta di Nizza (CDFUE), l'installazione e l'utilizzazione di impianti di video-

¹⁷ L. 3 dicembre 2021, n. 105.

sorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici di cui all'art. 4, numero 14, del citato regolamento (UE) 2016/679, in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, sono sospese fino all'entrata in vigore di una disciplina legislativa della materia e, comunque, non oltre il 31 dicembre 2023.¹⁸

Tuttavia, vi innesta, in virtù di quanto previsto dal comma 12, un'eccezione:

I commi 9, 10 e 11 non si applicano ai trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali ... in presenza, salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero, di parere favorevole del Garante ...

Il testo normativo si presenta oscuro, sembrando legittimare il ricorso agli strumenti di riconoscimento facciale, da parte dell'autorità giudiziaria, anche senza necessità del parere "amministrativo del Garante", necessario, invece, per le forze dell'ordine. Un approdo siffatto esporrebbe il sistema normativo a più di una censura, sul versante, tra gli altri, del principio di proporzionalità, non essendo neppure precisato per quale tipologia di reati possa attivarsi lo strumento in esame, della cui invasività non è dato dubitare, sotto il profilo della libertà morale dell'individuo, intesa come libertà di autodeterminazione, anche negli spazi pubblici.

Per fugare sospetti di incostituzionalità, si è suggerito¹⁹ di intendere l'art. 9, comma 12, quale regola "volta a ribadire che, anche al netto della moratoria generale nei confronti di tale apparato, le autorità di *law enforcement* possono continuare ad avvalersene, nei soli casi e con i limiti stabiliti dalle fonti sovraordinate e dal codice di rito". Pur accedendo a questa lettura, le incertezze non si dissolvono del tutto se si considera che la disciplina processual-penalistica non contiene

¹⁸ L'art. 8-ter del d.l. 10 maggio 2023, n. 51, coordinato con la l. 3 luglio 2023, n. 87, di conversione, ha spostato al 31 dicembre 2025 il termine originariamente previsto.

¹⁹ Della Torre 2023: 178.

alcuna disposizione tecnica per l'impiego di tali strumenti. È giunto il tempo che, a livello nazionale,²⁰ il legislatore si assuma la responsabilità di un chiaro intervento normativo che regoli modi e usi delle nuove tecnologie, nel rispetto delle garanzie fondamentali dell'individuo e dei principi di proporzionalità e accessibilità.

5. Le prospettive a livello europeo

Se guardiamo all'orizzonte europeo, nella Proposta di Regolamento²¹ avanzata dalla Commissione europea nell'aprile 2021 "che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione", la materia è collocata nel Titolo II dedicato alle "[p]ratiche di intelligenza artificiale vietate". Nello specifico, all'art. 5 § 1 lett. d) della proposta si afferma, in prima battuta, il generale divieto di impiego per finalità di *law enforcement* dei sistemi di identificazione biometrica in tempo reale in luoghi accessibili al pubblico, in quanto ritenuta particolarmente in-

20 Spunti interessanti si trovano nella Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI)), § 25: «prende atto dei diversi tipi di utilizzo del riconoscimento facciale, come, ma non solo, la verifica/autenticazione (abbinamento di un volto dal vivo a una foto in un documento di identità, per es. i bordi intelligenti), l'identificazione (ricerca della corrispondenza tra una fotografia e un database di immagini) e la rilevazione (individuazione di volti in tempo reale da fonti quali la televisione a circuito chiuso e ricerca di una corrispondenza con i database, per es. sorveglianza in tempo reale), ciascuna delle quali ha diverse implicazioni per la protezione dei diritti fondamentali; è fermamente convinto che la diffusione dei sistemi di riconoscimento facciale da parte delle autorità di contrasto dovrebbe essere limitata a finalità chiaramente giustificate nel pieno rispetto dei principi di proporzionalità e di necessità e della legge vigente; ribadisce che, come minimo, l'utilizzo della tecnologia di riconoscimento facciale deve essere conforme ai requisiti di minimizzazione dei dati, precisione dei dati, limite di conservazione, sicurezza e affidabilità dei dati, ed essere lecito, equo e trasparente e perseguire una finalità specifica, esplicita e legittima chiaramente definita nel diritto degli Stati membri o dell'Unione». V., anche, Consiglio d'Europa, *Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data*- Convention 108, *Guidelines on Facial Recognition*, 28 gennaio 2021, dove sono contenute delle indicazioni dirette al legislatore.

21 COM (2021) 206 final.

vasiva dei diritti e delle libertà delle persone interessate "nella misura in cui potrebbe avere ripercussioni sulla vita privata di un'ampia fetta della popolazione, farla sentire costantemente sotto sorveglianza e scoraggiare in maniera indiretta l'esercizio della libertà di riunione e di altri diritti fondamentali" (considerando n. 18). Le eventuali deroghe – ammesse a patto che i software superino lo scrutinio preventivo di conformità da parte di un ente certificatore terzo – sono circoscritte alle ipotesi contemplate dalla stessa disposizione in cui sia "strettamente necessario": "individuare specifiche vittime di reato" (i); prevenire "un'imminente minaccia alla vita o all'incolumità fisica degli individui o ... un attacco terroristico" (ii); o, infine, "individuare", "localizzare" o esercitare "l'azione penale" nei confronti dell'"autore" o di "colui che si sospetta sia tale" di uno dei reati riconducibili alle 32 categorie di fattispecie di cui alla decisione quadro 2002/584/CE istitutiva del MAE, e a patto che, sulla base della disciplina nazionale, tali reati siano "punibili" nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni" (iii). Nel successivo § 2, si aggiunge che l'utilizzo di questi sistemi dovrà inoltre essere calibrato sulla "natura della situazione" nonché sulle "conseguenze" che possono derivarne "per i diritti e le libertà di tutte le persone interessate", con particolare riguardo, nel primo caso, alla "gravità", alla "probabilità" ed all'"entità del danno causato dal mancato uso del sistema" (a) e, nella seconda ipotesi, alla "gravità", alla "probabilità" ed all'"entità" delle suddette conseguenze (b). Ancora, viene operato un riferimento esplicito alla necessità di stabilire limitazioni "temporali" e "geografiche", oltreché "personali", che siano "necessarie e proporzionate in relazione all'uso".

L'intento è evidentemente quello di 'blindare' la materia, con un primo vaglio di proporzionalità operato in astratto a livello eurounitario, vaglio che spetterà poi ai singoli ordinamenti nazionali declinare con "regole dettagliate che limitino" ulteriormente "l'esercizio di un potere tanto invasivo e impattante su beni giuridici supremi" nell'ipotesi in cui decidano di ammettere l'utilizzo di software di identificazione biometrica in tempo reale in luoghi accessibili al pubblico (§ 4).

Ma vi è di più: alle condizioni appena esaminate, la proposta affianca infatti un altro requisito che suona come una

conferma della definitiva presa di coscienza dell'estrema intrusività delle AFRTs. Invero, ogni singolo utilizzo delle tecnologie in questione deve essere preceduto dal rilascio di un'apposita autorizzazione da parte di un'autorità giudiziaria o di un'autorità amministrativa indipendente dello Stato membro, emessa a seguito di richiesta motivata e nel rispetto delle suddette regole nazionali dettagliate. Segnatamente, occorre accertare, sulla base di "prove oggettive" o "indicazioni chiare", la necessità e la proporzionalità della misura rispetto ad almeno una delle finalità ammesse. L'unica ipotesi in cui è consentito prescindere dall'autorizzazione riguarda eventuali situazioni di urgenza, salvo comunque l'obbligo di ottenere la convalida (§ 3).

Da questo breve quadro, appare chiaro come la Commissione abbia concepito il riconoscimento facciale automatizzato svolto in tempo reale alla stregua di un'"intrusion[e] significativ[a] nella sfera privata e dei dati personali" tutelati dagli artt. 7 e 8 CDFUE, che, in quanto tale, stando all'orientamento consolidato della Corte di Giustizia, deve non solo essere "regolat[a] da norme di legge, di modo che l'acquisizione per fini di prevenzione o di accertamento processuale sia circoscritta al ricorrere di reati sufficientemente gravi" e "contenuta nella misura strettamente necessaria per conseguire il fine perseguito", ma anche "accompagnata dal controllo preventivo di un giudice o di una entità amministrativa indipendente".

Invece, per quel che concerne i sistemi di identificazione biometrica da remoto, questi sono inquadrati tra i sistemi di IA ad alto rischio. Pertanto, il loro utilizzo deve rispettare una serie di condizioni, tra cui l'attuazione, per tutto il ciclo di vita del sistema, di un meccanismo di *risk-management* volto a individuare e minimizzare i rischi prevedibili prima della messa in commercio o emersi durante l'utilizzo, a cui si accompagnano contestuali obblighi di informazione al pubblico e di *testing* costante dei sistemi, nonché il rispetto di standard qualitativi dei dati che fungono da base per l'addestramento dei sistemi ad alto rischio al fine di contenere errori e discriminazioni. Un aspetto, quest'ultimo, particolarmente rilevante in relazione alle tecnologie di riconoscimento facciale, affette da pregiudizi di genere o legati al colore della pelle delle persone. Inoltre, si richiede che il sistema sia

"sufficientemente trasparente", così da permettere di comprendere come funzioni il meccanismo di apprendimento della macchina, e che assicuri un'efficace supervisione umana. Infine, tali sistemi dovranno sottostare a una procedura di verifica di conformità a standard e regole stabilite dall'Unione, che potrà essere effettuata dal produttore stesso o da un organismo certificatore terzo.

Sul diverso versante della cooperazione giudiziaria, l'8 aprile 2022 il Consiglio europeo ha approvato la proposta di Regolamento sullo scambio di dati automatizzato per scopi di cooperazione transfrontaliera nella lotta alla criminalità e al terrorismo.²² La proposta – denominata 'Prüm II' – intende aggiornare il cd. quadro di Prüm, un corpo di decisioni, adottate nel 2008, con l'obiettivo di sostenere la cooperazione giudiziaria e di polizia a livello transfrontaliero in relazione a questioni penali, prevedono lo scambio automatizzato di dati specifici (dati relativi a profili DNA, impronte digitali e immatricolazione di veicoli) tra le autorità competenti per la prevenzione, l'indagine e l'accertamento di reati. Secondo quanto previsto dagli artt. 35 e seguenti del testo, le banche dati detenute dalle singole autorità di sicurezza degli Stati membri non confluiranno in un unico *database* centrale a livello europeo, ma le singole piattaforme nazionali saranno collegate attraverso la creazione di router centrali, "al fine di facilitare l'instaurazione di connessioni tra gli Stati membri e con Europol per l'interrogazione e l'estrazione dei dati biometrici e l'assegnazione di un punteggio alle relative corrispondenze in conformità del presente regolamento". In sostanza, le autorità di pubblica di sicurezza avranno la possibilità di interrogare il *router* europeo trasmettendo uno o più dati biometrici (DNA, immagini facciali e dati dattiloscopici) relativi ad un certo soggetto. Ricevuta la richiesta, il *router* invierà la domanda di interrogazione agli Stati membri, i quali provvederanno ad interrogare le proprie banche dati "in modo automatizzato e senza indugio". Una volta ricevuti eventuali riscontri positivi da parte di una o più banche dati, il *router* classificherà le risposte in base al punteggio della cor-

22 Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio sullo scambio automatizzato di dati per la cooperazione di polizia ('Prüm II'), che modifica le decisioni 2008/615/GAI e 2008/616/GAI del Consiglio e i regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818 del Parlamento europeo e del Consiglio, 8 dicembre 2021.

rispondenza, inviando all'autorità pubblica richiedente l'elenco dei dati biometrici per i quali è stata riscontrata una corrispondenza e i relativi punteggi. Inoltre, all'interno dell'informazione condivisa dalle polizie rientreranno anche le immagini facciali, così come verrà data la possibilità di utilizzare algoritmi di riconoscimento facciale per automatizzare la fase di riconoscimento: tramite questi algoritmi, sarà possibile confrontare le immagini catturate da telecamere a circuito chiuso con le foto di social network o contenute nei telefoni di una vittima con le foto segnaletiche contenute nei database della polizia.

Questo tipo di struttura, pur con i vantaggi che presenta sul piano del potenziamento dell'attività investigativa, tuttavia, non è immune da critiche sul versante della mancanza di sufficienti garanzie per gli individui in ordine al principio di proporzionalità.²³ Manca una precisa indicazione degli elementi essenziali sottoposti allo scambio di dati come, ad esempio, le tipologie di reati che possano giustificare una richiesta. Ne consegue che sarebbe legittimo accedere ai dati biometrici di un individuo (DNA e mappatura del volto) anche solo per il perseguimento di reati minori; inoltre, non è neppure chiaro se il database contenga dati anche delle vittime e dei testimoni.

Queste brevi note dimostrano come la materia del riconoscimento facciale e, in linea generale, le interazioni tra il processo penale e l'intelligenza artificiale siano in costante evoluzione.²⁴ Ciò richiede un elevato livello di attenzione da parte di tutti gli operatori per evitare di dovere ricorrere – come avvenuto in Giappone – all'uso delle maschere al fine di sottrarsi a forme illegittime di “sorveglianza di massa”.

Bibliografia

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

23 European Data Protection Supervisor, Opinion 4/2022, on the Proposal for a Regulation on automated data exchange for police cooperation ('Prum II'), 2 marzo 2022.

24 Quattrocchio: 2020.

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*, 9/2022, 23-44.

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.

Della Torre 2023: Della Torre J., *Algoritmi di facial recognition e procedimento penale italiano*, in Micheli I. (a cura di), *Ragioni Comuni 2019 – 2020. Risultati delle attività progettuali realizzate tramite assegni di ricerca finanziati dalla Regione Friuli Venezia Giulia ai sensi della LR 34/2015, art.5, c. 29-33*, Trieste 2023, 167-181.

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

Mobilio 2021: Mobilio G., *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli 2021.

Quattrocchio 2020: Quattrocchio S., *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Cham, 2020.

Rodotà 2003: Rodotà S., *Relazione 2003. Discorso del Presidente Rodotà*, in www.garanteperlaprivacy.it

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

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.