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.

PARTE I

LA PROVA DEL DNA NEL PROCESSO PENALE

INTRODUZIONE: 120 ANNI DI POLIZIA SCIENTIFICA

Pasquale Alongi
Gabinetto Regionale di Polizia Scientifica di Catania

Nel 2023 la Polizia di Stato celebra i 120 anni di Polizia Scientifica. Al fine di ripercorrere le tappe che hanno portato alla sua istituzione, abbiamo immaginato di intervistare il Professore Salvatore Ottolenghi, fondatore della Scuola di Polizia Scientifica. Nato ad Asti nel 1861, Ottolenghi si laureò in medicina e chirurgia a soli 23 anni, nel 1884, presso l'Università di Torino e fu allievo di Cesare Lombroso di cui divenne assistente occupandosi di antropologia e psichiatria.

Erano anni di grande fermento in Europa, le scienze forensi stavano facendo il loro ingresso nelle aule dei tribunali diventando strumento imprescindibile per le indagini di Polizia Giudiziaria.

Il 2 aprile del 1903 è una data epocale per l'allora Corpo delle Guardie di Pubblica Sicurezza e per la Polizia di Stato: comincia il primo corso di formazione per funzionari di Polizia che avrebbero prestato servizio presso le articolazioni della Polizia Scientifica.

Oggi l'analisi della scena di un crimine e la prova scientifica rappresentano elementi indispensabili per la verifica di ipotesi investigative e l'individuazione dei possibili autori. L'attività è 'scientifica' perché si applicano le metodologie tipiche dell'attività della scienza: si osserva, si raccolgono i dati, si formula una ipotesi, si verifica l'ipotesi con un esperimento, si dà certezza della veridicità dell'ipotesi. Il primo ad applicare il metodo scientifico alle indagini di Polizia è stato, appunto, il prof. Ottolenghi che nei primi anni del '900 ha 'inventato' la Polizia Scientifica, creando un modello esportato in tutto il mondo.

Per meglio capire e contestualizzare le idee del prof. Ottolenghi e la sua intuizione, facciamo dire a lui come è riuscito a dare alla Polizia un'impostazione 'scientifica'. L'intervista che segue è tratta da A. Giuliano, *Salvatore Ottolenghi. Le impronte digitali in Polizia Scientifica e Medicina Legale*, Torino, 2018.

Prof. Ottolenghi, lei è senza dubbio il fondatore della Polizia Scientifica. Si deve a lei la creazione della scuola della Polizia Scientifica e la connessa attività che di fatto ha portato all'istituzione del Servizio di Polizia Scientifica all'interno del Dipartimento della Pubblica Sicurezza. La prima domanda che le faccio è questa: perché ha riscontrato la necessità di organizzare un corso di Polizia Giudiziaria Scientifica?

"Sono stato indotto specialmente dall'abisso che vedevo esistere fra verità scientifiche e praticità nel campo della Polizia, sorpreso di vedere così poco utilizzate le nuove conoscenze sulla natura dei rei e quindi pensai di promuovere un corso libero universitario ... Subito intravidi le speciali applicazioni che la criminologia scientifica e la medicina legale, col loro speciale tecnicismo, potevano e dovevano apportare al funzionamento obbiettivo della Polizia giudiziaria".

Lei ha organizzato il primo corso di Polizia Scientifica per funzionari del Corpo delle Guardie di Pubblica Sicurezza che si tenne a Roma con la prima lezione il 2 aprile del 1903. E allora le chiedo, perché un medico, uno scienziato come lei, ha avuto l'ardire di guardare alla Polizia Scientifica e allo studio criminologico dei reati?

"Perché? Perché ... van gettandosi le basi di una vera Polizia Scientifica e se ne disegna almeno vivamente il bisogno. Noi abbiano fatto, fin ora, la Polizia così come si faceva la guerra nei tempi eroici, tutt'a casaccio, ad empirismo, salvo il merito individuale in astuzia e forza muscolare di alcuni pochi che decidevano spesso della vittoria.

Abbiamo dei questori che sono e si dicono abili, come erano abili Ulisse ed Achille; ma non ne abbiamo nessuno che ... fondi le sue indagini sulle basi scientifiche offerte dagli studi nuovi di statistica, di antropologia criminale, che moltiplichi, insomma, il proprio impegno, colle forze enormi e, quel che è piu, esattamente governabili, dalla scienza".

Professore, può spiegarci come ha organizzato il suo corso di Polizia Scientifica?

"Ma certo ...

La prima parte sarà dedicata alla ricerca del delinquente ... qui dedicheremo i migliori metodi di segnalazione ... per il riconoscimento. La seconda parte dovrà occuparsi

della istruttoria del procedimento specialmente del modo a procedere negli interrogatori. In terza parte seguiremo l'imputato nelle cause penali. Mi estenderò a lungo in questo corso sulla preparazione di quei servizi che, come dimostrerò, sono assolutamente necessari e dovranno costituire la vera forza strategica della Polizia e dell'autorità giudiziaria. Ma queste istruzioni non si possono formare con circolari-progetti; la loro applicazione è intimamente connessa all'istruzione e riforma del personale e a quel complesso innovamento dei mezzi di lotta che si deve assolutamente effettuare perché la Polizia giudiziaria si rinnovelli e rinvigorisca poggiandosi su basi scientifiche".

Secondo lei qual è la necessità di riformare le attività di Polizia e di avere una Polizia Scientifica?

"Assistiamo a una situazione fallimentare … nel 1894 nel periodo dell'istruttoria la metà circa degli imputati fu prosciolta per insufficienza di prove … il 28% venne prosciolto per non provata reità. La Polizia dovrebbe essere la più grande tutela della sicurezza della società ed invece … essa ne previene sufficientemente, salvo eccezioni, assicura l'arresto del colpevole".

Professore, come è riuscito a convincere i vertici della Polizia della necessità di istituire la Polizia Scientifica?

"Il 4 giugno del 1902, senza alcuna presentazione, andai a bussare alla porta del Capo della Polizia – Direttore Generale della Pubblica Scurezza, Francesco Leonardi, e gli esposi il mio programma teorico e soprattutto pratico di Polizia Scientifica. Questi lo accolse con tanto ardore da presentare subito a Giolitti il progetto. Il giorno dopo, fui convocato dal Leonardi, il quale, quasi incredulo del successo ottenuto, mi comunicò che Giolitti dispose di organizzare immediatamente il corso. Fu così che nel 1902 si tenne a Roma presso la sala dei riconoscimenti del carcere di regina Coeli, il primo corso di Polizia Scientifica, al quale parteciparono 35 funzionari di pubblica sicurezza e durò 3 mesi, dall'ottobre al dicembre del 1902. Fu la nascita della Scuola di Polizia Scientifica".

Quindi il corso del 1902 fu il primo corso di Polizia Scientifica?

"In effetti no. Quello che definiamo il primo corso, ebbe inizio il 2 aprile del 1903. Nella Scuola organizzai tre servizi operativi: Servizio di Segnalamento e identificazione; Servizio di investigazione tecniche di Polizia Giudiziaria; Servizio antropologico-biografico. Non era solo un luogo di istruzione, ma divenne un posto in cui occuparsi di questioni giudiziarie di Polizia anche perché si faceva rielevante il problema del metodo da utilizzare per riconoscere i criminali fissando le loro generalità a caratteri da dirsi invariabili nel corso della loro vita".

E cosa successe dopo l'istituzione della scuola, quali furono gli effetti pratici di avere dei funzionari di Polizia Scientifica sul territorio italiano?

"Cambiò il modo di fare Polizia Giudiziaria. Nel 1911 la possibilità di prendere le impronte ai delinquenti era presente in 21 Gabinetti segnaletici, in 49 Uffici provinciali, in 6 Uffici Circondariali, in 10 Uffici di Commissariato presso le direzioni compartimentali delle ferrovie dello stato, in 61 case penali e in 43 Carceri giudiziari".

Professore, da dove nasce l'idea di avere la certezza dell'identità personale di un soggetto?

"Tutti gli uomini hanno uno o più caratteri propri che li contraddistinguono dagli altri della spessa specie e che sono sufficienti a fissare l'identità di essi. In natura non esistono due cose uguali. L'uguaglianza esatta esiste solamente in matematica. Quando di una persona abbiamo i caratteri e ne conosciamo il nome, possiamo dire che la persona è identificata nel vero senso della parola. Alle funzioni di Polizia occorre un segnalamento che si faccia rapidamente e si abbisogni di particolari strumenti misuratori che conduca all'identificazione esatta".

Ci può fare un esempio pratico?

"Il 18 febbraio 1911 la Questura di Genova arrestava per furto una sedicente suddita francese, tale Annet Boluert, e ne trasmetteva il cartellino al mio ufficio, presso il casellario centrale di Roma. Con le impronte digitali venivano subito qui rinvenuti i precedenti di detta donna che era stata arrestata a Vienna sotto il nome Erica Lerchel, a Milano sotto il nome di

Anna Francesca Limberti, a Roma sotto il nome di Federica Libertini e a Ventimiglia sotto il nome di Eleonora Ambrosini.

In tal modo la sedicente Annet Boluert, che a Genova avrebbe potuto passare per impregiudicata, è stata presentata all'autorità giudiziaria con tutto il corredo completo della sua abbondante recidiva specifica, disseminata sotto vari nomi in Italia ed all'estero.

Vede, mentre il nostro paese era nel 1902 alla coda delle altre nazioni in questo campo, esso possiede ora il servizio forse meno fastoso ma più pratico. In nessuna nazione ove si hanno servizi centrali superbi si è raggiunta la diffusione che ha assunto nella nostra terra, gli uffici di segnalamento sono in condizione di collaborare giornalmente con tutti gli altri posti di segnalamento del Regno.

In Italia ho creato la prima scuola ufficiale di tal genere nel mondo. Non esisteva e non esisterà neanche per diversi anni, nessun paese con una istituzione così organizzata e inserita all'interno della Polizia, in maniera che ogni evoluzione scientifica potesse immediatamente essere riversata nella pratica di Polizia Giudiziaria".

Quale fu la prima volta che l'attività della Polizia Scientifica ha risolto un caso importante?

"Il 22 marzo 1909, Roma via Frattina. In una camera d'affitto al 6° piano, viene ritrovato il cadavere di un uomo all'interno di un baule. La mia squadra si recò sulla scena del crimine su richiesta del giudice istruttore. Giovanni Gasti, dopo aver fissato con lastra fotografica le condizioni del reato, procedette al segnalamento descrittivo del cadavere e provocava successivamente il concorso dell'intervento del commissario Umberto Ellero per il segnalamento fotografico e del delegato dr Giuseppe Falco per il segnalamento dattiloscopico e antropometrico. La scuola trasmise subito le impronte e le misure antropometriche agli uffici di Polizia esteri, nella speranza di trovare un riscontro per aiutare gli inquirenti a trovare una pista. Quando sembrava persa ogni speranza, la questura di Roma il 30 aprile, comunicava che per la Polizia di Varsavia, con i dati che aveva ricevuto dalla mia scuola, soprattutto a mezzo delle impronte digitali, l'individuo era stato riconosciuto per Edmondo Tarantovich. Le indagini della

scientifica portarono dritto ad una pista internazionale, un regolamento di conti tra spie estere in Italia".

Professore, in quale modo riuscì a divulgare le innovazioni e le scoperte della metodologia della scientifica in tutta Italia?

"Nel 1910 dotai la scuola di una pubblicazione ufficiale: Il bollettino della scuola di Polizia Scientifica e del servizio di fotosegnalamento. Questo bollettino servì come diffusore delle conquiste e dei traguardi raggiunti dalla scuola. Informando tutti gli uffici di tutti gli ultimi ritrovati, dei casi risolti per diffondere sul territorio la validità e la qualità dei metodi scientifici".

Lei ha inventato anche le modalità di effettuare il sopralluogo?

"Certamente".

Può dirci qualcosa a riguardo?

"Il mio metodo descrittivo che ho definito 'il ritratto parlato del sopralluogo' serve a indicare precipuamente le modalità da utilizzare. Con la circolare del Guardasigilli Fani del 24 luglio 1910, si dispose che i giudici istruttori possono avvalersi del personale della scientifica nella scena del crimine. Il sopralluogo ora è una attenta descrizione dell'ambiente condotta con una serie di regole e una terminologia accuratamente codificata per rendere certe e uniformi le relazioni effettuate sulla scena del crimine. I nostri funzionari imparano a procedere nei sopralluoghi in modo che nulla rimanga inosservato, nulla venga disperso o manomesso. Imparano a rilevare le impronte poco visibili o invisibili, imparano a riprodurre con la fotografia le parti essenziali, la posizione di un cadavere, l'insieme di un ambiente. Imparano infine a redigere rapporti completi obbiettivi, onde possano costituire la base fondamentale del procedimento istruttorio. Il funzionario della Polizia Scientifica deve rimanere indifferente a qualsiasi intuizione personale".

Quindi la sua scuola fu un esempio per la Polizia di tutto mondo?

"Il primo tangibile consenso l'ho raccolto in occasione del V° congresso di psicologia tenutosi a Roma nel 1905, quando i congressisti stranieri manifestarono tutta la loro ammirazione per i risultati conseguiti. Ma non fu tutto merito mio. Non avrei raggiunto lo scopo propostomi senza l'opera preziosa dei miei collaboratori: Giovanni Gasti ideatore la classificazione dattiloscopica che poi ci hanno copiato in tutto il mondo. Giuseppe Falco medico legale pel fotosegnalamento descrittivo dattiloscopico e antropometrico; e Umberto Ellero che inventò un sistema per fotografare i soggetti, con due macchine fotografiche di talché si aveva su di una stessa foto, sia il fronte che il profilo".

Professore, è vero che il suo metodo, per fotosegnalare le persone e il metodo descrittivo del sopralluogo giudiziario ebbe successo anche in altri paesi?

"Il 13 maggio del 1925 partecipai a New York alla conferenza internazionale di Polizia. La fondazione della scuola di Polizia Scientifica con i suoi programmi e l'inaugurazione del nuovo Istituto di medicina legale, erano già conosciuti in tutto il mondo. Così quella sera mostrai le proiezioni fotografiche di dieci casi pratici seguite con la massima attenzione dai presenti. Spiegai ampiamente i vari casi ottenuti.

In America non si fanno chiacchere. E quando io ho presentato questa mia relazione al Direttore della Polizia signor Enright, si è preoccupato che non fosse altro che un'esposizione dottrinale. «Qui in America siamo in America e vogliamo fatti», mi ha detto. «In realtà, caro signore, lei parla con uno scienziato e con un pratico che lotta da 25 anni contro due cose: contro il misoneismo e contro i pregiudizi antiscientifici». Il direttore della Polizia d'America affermò che avrebbe accolto con simpatia la 'Polizia Scientifica', ma che avrebbe voluto vedere dei fatti. Noi gli abbiamo risposto che in quanto a fatti ne abbiamo tutti i giorni poiché la nostra è una Polizia pratica. Avevo con me delle proiezioni che ricordavano dei sopralluoghi fatti dai miei collaboratori. Ogni presentazione cominciava con «I will show in this slide ...» come del resto si fa anche oggi.

È stata la scintilla che ha provocato l'incendio. Sono stato intervistato dal capo dell'ufficio stampa della Polizia ameri-

cana. Questa intervista è durata più di due ore e ha determinato il successo completo. Il capo dell'ufficio stampa è rimasto ammirato dinanzi alla dimostrazione pratica dei risultati splendidi conseguiti dalla nostra scuola. E la mia relazione e le proiezioni hanno ottenuto nella seduta destinata a noi, il plauso e il consenso generale. Dopo la mia relazione, il presidente del convegno Enright disse che ero un 'very remarkable man', ed espresse a nome di tutti i convenuti, l'ammirazione viva e sincera per quanto l'Italia ha compiuto nel campo della Polizia Scientifica e della criminologia, proclamando che se la Polizia americana vorrà proseguire sulla via del progresso, dovrà seguire l'Italia!".

Professore Ottolenghi un'ultima domanda prima di congedarla. Cosa è stato fatto per la scientifica?

"È stato fatto molto ma c'è ancora tanto da fare ...".

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

Paola Di Simone
Gabinetto Regionale di Polizia Scientifica di Palermo – Laboratorio di Genetica Forense

Abstract: Forensic genetics, based on the analysis of highly variable DNA regions, is a useful tool in criminal investigations. Any item with biological traces or a biological trace itself, collected from a crime scene, can be analysed in order to know who deposited that trace. Of course, it is always important and necessary to evaluate the context. DNA analysis and also its way of inheritance allows the identification of human remains, victims of mass disasters and missing persons. A very useful tool is the National DNA Database.

Parole chiave: genetica forense; tracce biologiche; identificazione; banca dati del DNA.

1. Premessa

L'esigenza di applicare un metodo scientifico per l'identificazione dell'autore di un crimine – ove per crimine si intende qualsiasi fattispecie di reato – o per ricostruirne la dinamica, maturò nella seconda metà dell'Ottocento.

Nel 1870, in Francia, il criminologo Alphonse Bertillon fondò il primo laboratorio di identificazione criminale e sviluppò un sistema di riconoscimento biometrico basato su misurazioni delle caratteristiche antropometriche[1] dopo il ventesimo anno di età in quanto ritenne che proprio in quello specifico periodo l'ossatura non cambia in maniera significativa. Il metodo in questione venne applicato dapprima ai detenuti e, successivamente, tale approccio identificativo, che prese il nome di 'sistema Bertillon' o 'Bertillonage', venne adottato in Europa e negli Stati Uniti. Tuttavia, nel giro di pochi anni, il sistema si dimostrò fallace per le difficoltà che emersero nel

1 Si fa riferimento alle misure fisiche di una persona prendendo in considerazione vari elementi quali il cranio, la lunghezza degli arti, la lunghezza delle dita e dei piedi, la lunghezza del naso, ovvero anche le caratteristiche dell'orecchio.

momento di prendere tali misurazioni in modo oggettivo e preciso, oltre che per il verificarsi di un grave errore giudiziario. Così, Bertillon introdusse nella prassi per l'identificazione del criminale anche la foto segnaletica, sia frontale che laterale dell'individuo a mezzo busto, segnando di fatto l'inizio del fotosegnalamento. Inoltre, Alphonse Bertillon comprese l'importanza della 'ricerca delle tracce' all'interno di una scena del crimine: è sua la celebre frase "la traccia è il biglietto da visita del criminale, un testimone silenzioso che non mente mai".

In Italia, in quegli stessi anni e sulla scorta del positivismo francese, maturò un grande interesse per le scienze forensi e, sotto la guida di Cesare Lombroso,[2] vennero avviati i primi studi sulla criminalità e l'antropologia criminale.

Nell'ottica di voler ripercorrere brevemente le tappe che oggi consentono ai laboratori della Polizia Scientifica italiana di avvalersi delle più moderne strumentazioni e tecnologie in tutti gli ambiti delle scienze forensi, non si può non citare il Prof. Salvatore Ottolenghi[3] che, per primo in Italia, istituì nel 1903 il '1° Corso di Polizia Scientifica', creando le premesse per la nascita della Scuola di Polizia Scientifica. Ancora oggi, a distanza di 120 anni, vengono qualificati ogni anno "Operatori di Polizia Scientifica', e si svolgono periodicamente corsi di formazione, aggiornamento e addestramento per conferire a tutti coloro che lavorano all'interno della Polizia Scientifica le competenze necessarie per svolgere al meglio le proprie attività.

Durante la seconda metà dell'800 si affacciò, nel mondo delle scienze applicate alle indagini di polizia giudiziaria in ottica identificativa, l'approccio basato sull'analisi dell'impronta digitale che, ancora oggi, è considerata una della 'prove regina' all'interno delle aule dei tribunali. Il tema delle impronte digitali verrà affrontato in altra sezione del presente volume; tuttavia, è doveroso citare il primo caso giudiziario risolto con l'impiego dell'impronta digitale al fine di comprendere la distanza temporale che intercorre tra questo approccio e l'avvento della genetica forense.

2 Cesare Lombroso (1835-1909), psichiatra e antropologo, è considerato il padre della criminologia moderna.

3 Salvatore Ottolenghi (1861-1934), medico legale, allievo e poi collaboratore di Cesare Lombroso, fondatore della Scuola di Polizia Scientifica.

È il 1892 quando in Argentina la polizia indentifica un'infanticida, una madre, che con il sangue delle piccole vittime, il figlio di sei anni e la figlia di soli quattro, aveva impresso su una superficie la propria impronta digitale, la propria firma.

Bisogna aspettare quasi un secolo prima che venga introdotta nel mondo delle scienze forensi la prova del DNA utilizzata in ottica identificativa. Infatti, è solo nel 1984 che nasce il DNA *fingerprint*, l'impronta genetica.

2. La genetica forense

La genetica forense, pensata come approccio scientifico per l'identificazione dell'autore di un crimine, affonda le sue radici nel principio che il DNA è presente in maniera identica – ad esclusione dei mosaici genetici o dei soggetti sottoposti a trapianti di organi –, in tutte le cellule del nostro corpo, salvo i globuli rossi, poiché privi di nucleo. Sebbene il 99.9% del nostro DNA sia identico all'interno del genere umano, è proprio il restante 0.1% che rende ciascun individuo geneticamente unico, con l'unica eccezione dei gemelli monozigoti. Questa frazione di DNA altamente variabile risulta di particolare interesse per i genetisti forensi.

La possibilità di potere 'discriminare' e differenziare gli individui sulla base di alcune caratteristiche genetiche era nota già dai primi del 1900: risale, infatti, al 1901 la scoperta dei gruppi sanguigni che furono impiegati in rudimentali indagini in ambito forense, se non altro ai fini di esclusione, dato il loro scarso potere discriminativo.[4] A seguito di tale scoperta, furono avviati diversi studi che consentirono di individuare differenti varianti di proteine e si iniziò a parlare di polimorfismi.[5] L'analisi dei gruppi sanguigni e delle proteine caratterizzò il mondo della biologia forense fino al 1984 quando, Alec Jeffreys, nel suo laboratorio presso l'Università di Leicester, per primo individuò dei tratti di DNA che presentavano

4 Si pensi a quanti individui condividono lo stesso gruppo sanguigno.

5 Il polimorfismo in biologia si verifica quando due o più fenotipi diversi esistono contemporaneamente in almeno l'1% degli individui nella stessa popolazione. Per polimorfismo genetico si intende una variazione della sequenza del DNA in almeno l'1% della popolazione.

similitudini, ma anche differenze, tra i vari membri della famiglia di un suo tecnico; ecco allora che i polimorfismi genetici entrarono nel mondo delle scienze forensi. Inutile dire che la scoperta fu considerata rivoluzionaria e pose le basi, con tecniche ancora rudimentali se paragonate a quelle attuali, per un nuovo capitolo della genetica forense.

La tecnica messa a punto da Jeffreys, che prese il nome di DNA *fingerprint*, fu utilizzata per la prima volta in un caso, molto contestato, di immigrazione. Il 'nuovo' strumento fece il proprio debutto in un'indagine di polizia volta ad identificare l'assassino di due adolescenti, Lynda Mann e Dawn Ashworth, rapite e uccise nei vicini villaggi di Narborough e Enderby rispettivamente nel 1983 e nel 1986. L'autore del duplice omicidio, Colin Pitchfork, fu identificato attraverso l'analisi comparativa tra il DNA *fingerprint* ottenuto da un suo campione di sangue con quello ottenuto dall'analisi delle tracce di liquido seminale trovate sui corpi delle vittime. Nel 1988, sulla sola base del riscontro scientifico, Colin Pitchfork fu condannato.[6]

Anche in Italia si comprende l'importanza del DNA come prova a fini identificativi per le indagini di polizia giudiziaria. Sono trascorsi pochi anni dal DNA *fingerprint* di Alec Jeffreys e, sulla falsariga dell'esperienza inglese, viene istituito il primo laboratorio di genetica forense nella sede centrale della Polizia Scientifica di Roma. Tra i tanti reperti analizzati fin da quegli anni presso la struttura della Polizia Scientifica figurano anche i mozziconi di sigaretta sequestrati in occasione del sopralluogo effettuato, il 23 maggio del 1992, nei pressi del casolare antistante l'autostrada all'altezza di Capaci.

3. La genetica forense e i laboratori di Polizia Scientifica

Oggi la genetica forense rappresenta un'importante risorsa per confermare ipotesi investigative o, come altrettanto spesso accade, per confutarle escludendo la presenza di un soggetto in un contesto ove si sia verificato un crimine.

6 Un dato curioso è che per il duplice omicidio delle due giovani, in una prima fase delle indagini, si autodenunciò del fatto di reato un giovane, Richard Buckland, che però fu poi scagionato proprio sulla base del DNA.

La Polizia Scientifica conta, attualmente, sei laboratori di genetica forense ubicati rispettivamente a Torino, Milano, Napoli, Palermo e Roma, ciascuno con una competenza territoriale extraregionale[7]. Tutti i laboratori di genetica forense della Polizia Scientifica sono accreditati 'ISO/IEC 17025': si tratta di una norma in grado di certificare le competenze di un laboratorio di prova, ratificando che il risultato di un'analisi – la cd. prova – risponda ai requisiti della norma e sia conforme a quanto prescritto da un metodo validato. L'accreditamento ISO/IEC 17025 rappresenta inoltre un requisito cogente ai fini della produzione di profili genetici idonei per l'inserimento all'interno della Banca Dati Nazionale del DNA.

L'attività principale dei laboratori di genetica forense della Polizia Scientifica riguarda l'analisi di reperti prelevati dalla scena del crimine al fine di ottenere un profilo genetico che sia utile in ottica comparativa. I protocolli, ritenuti oggi attendibili dalla comunità scientifica internazionale che lavora nel settore, consentono di ottenere risultati da tutti i tipi di matrice biologica, indipendentemente dal substrato su cui essa è depositata. È pertanto possibile ottenere un profilo genetico dal sangue, dal liquido seminale, dalla saliva, dalle formazioni pilifere, dalle ossa, dai denti, da un determinato muscolo o ancora dalle cellule epiteliali di sfaldamento. Nel caso di campioni per i quali si presume la presenza di sangue, saliva o liquido seminale, viene sempre eseguita, in via preliminare, un'analisi finalizzata a confermare la tipologia della traccia. Questo test preliminare risulta di fondamentale rilevanza ai fini della contestualizzazione della prova soprattutto nel caso di omicidi e/o lesioni (per il sangue) e violenze sessuali (per liquido seminale e/o saliva).

Presso i laboratori di genetica forense, così come avviene anche in fase di sopralluogo, è possibile approfondire la ricerca di tracce biologiche latenti attraverso l'utilizzo di 'lampade a luce U.V.' particolarmente indicate, a specifiche lunghezze d'onda, per la ricerca di fluidi biologi non visibili ad occhio nudo – quali saliva, liquido seminale, urina, essudati – oppure me-

7 Competenze territoriali dei suddetti laboratori: Torino (Piemonte, Valle d'Aosta e Liguria); Milano (Lombardia e Triveneto); Napoli (Campania, Basilicata, Molise e Puglia); Palermo (Sicilia e Calabria); Roma I (Lazio e Umbria) e Roma II (Toscana, Emilia Romagna, Marche, Abruzzo e Sardegna)

diante l'uso di reagenti chimici – quali il 'luminol', il 'bluestar' o analoghi – nel caso si vada alla ricerca di tracce ematiche latenti, quali ad esempio quelle su indumenti o superfici lavate.

Oltre che nell'ambito delle attività di polizia giudiziaria, le caratteristiche intrinseche dell'analisi dei polimorfismi del DNA ed il fatto che viene ereditato per ciascuno di noi dai propri genitori, lo rendono un importante strumento a fini identificativi anche nell'ambito di riconoscimento di persone scomparse, cadaveri, vittime di disastri di massa; inoltre, tenendo presente proprio il carattere della 'ereditarietà del DNA', l'analisi dello stesso potrebbe essere fondamentale in tutti quei casi in cui risulta necessario eseguire dei test di paternità.

4. La genetica forense nelle indagini della Polizia giudiziaria

Come si è già detto, l'attività principale dei laboratori di genetica forense della Polizia Scientifica è quella di fornire un supporto alle attività investigative per individuare l'autore di un reato e/o ricostruirne la dinamica. Alla luce dei progressi della scienza nel campo della genetica forense e della individuazione di marcatori genetici con elevato potere discriminativo risulta di estrema rilevanza, nell'ambito di una indagine, la possibilità di ottenere profili genetici da poter comparare con eventuali profili genetici ottenuti da campioni biologici prelevati a soggetti di interesse.

L'approccio basato sull'analisi di tracce biologiche prelevate dalla scena di un crimine è particolarmente utile per i casi di criminalità diffusa. I furti, ad esempio, sono spesso caratterizzati dal ferimento del ladro che, lasciando delle tracce ematiche sul luogo del delitto, di fatto lascia la propria firma biologica. La presenza di una traccia ematica di un soggetto 'non avente titolo' all'interno di un appartamento, di per sé rappresenta un importante elemento probatorio in sede processuale. Se poi il ladro è recidivo, anche in assenza di sviluppi investigativi in grado di individuare il possibile autore, è possibile ricostruire eventuali episodi seriali attraverso i riscontri forniti dalla 'Banca Dati Nazionale del DNA'.

La possibilità di attribuire il profilo genetico ottenuto da una traccia ematica nei casi di lesioni, risse, accoltellamenti, omicidi tentati o consumati, può consentire di ricostruire la dinamica del crimine o, rifacendosi al principio di Locard[8] secondo il quale "ogni contatto lascia una traccia", fornire elementi utili per le indagini.

L'analisi di tracce di liquido seminale eventualmente presenti su tamponi effettuati su una (presunta) vittima, indumenti e/o lenzuola, e la possibilità di attribuire o escludere tale matrice biologica a un determinato soggetto possono fornire un importante riscontro nei casi di presunti abusi sessuali. Occorre chiarire, tuttavia, che in questo caso il riscontro si ferma all'attribuzione, o all'esclusione, della traccia ad un determinato soggetto. Il genetista forense, sulla base dell'analisi effettuata, nulla può dire sulla dinamica, cioè non può fornire alcuna indicazione circa la consumazione di un eventuale abuso, sulle circostanze, né tantomeno sull'intenzionalità o eventuale consensualità.

La prova del DNA risulta efficace anche nelle indagini contro la criminalità organizzata. L'analisi di armi utilizzate per rapine, atti intimidatori, omicidi, così come eventuali oggetti per i travisamenti – quali passamontagna o altri indumenti per travestimenti che spesso richiamano uniformi delle forze dell'ordine o guardie giurate – consente di ottenere profili genetici riconducibili a soggetti di particolare interesse investigativo.

Nel caso della tipologia di reperti sopra menzionati e quando si parla di criminalità organizzata, non si esclude un uso promiscuo degli stessi. A differenza delle impronte digitali dove l'eventuale sovrapposizione rende inutilizzabile a eventuali fini comparativi l'impronta evidenziata, in genetica forense è possibile ottenere un 'profilo genetico misto' riconducibile a più di un individuo; in taluni casi, con dei criteri stabiliti da linee guida internazionali, il profilo genetico misto può essere utilizzato a fini comparativi, ma non identificativi stante la miscellanea di più soggetti contributori.

L'eventualità in questione rende necessario l'impiego di valutazioni anche di tipo statistico per calcolare la probabilità che

8 Edmond Locard (1877-1966), criminologo francese, uno dei padri della scienza forense, elaborò il principio di interscambio.

un soggetto di interesse possa essere considerato contributore della mistura rispetto alla possibilità che ad aver contribuito alla genesi del profilo genetico in questione possa essere un altro individuo preso a caso in una popolazione di riferimento.

Inoltre, gli accertamenti genetico-forensi vengono spesso condotti su oggetti prelevati all'interno di presunti covi di latitanti al fine di ricostruire la rete di connivenze e risalire ai favoreggiatori. A tal proposito, nel 2010, nel corso delle indagini per la cattura di Giuseppe Falsone vennero perquisiti due covi nell'agrigentino: dall'analisi di alcuni reperti[9] prelevati da ciascuno dei covi si ottenne un unico profilo genetico che, dopo l'arresto a Marsiglia, fu comparato con quello del latitante ed a lui attribuito.

Pertanto, il riscontro basato sugli accertamenti genetico forensi risulta di grande utilità nelle indagini giudiziarie e talvolta dirimente nel caso di omicidi, femminicidi, infanticidi e matricidi, giusto per citare alcuni esempi.

Inoltre, come detto, i laboratori di genetica forense della Polizia Scientifica svolgono test di paternità nell'ambito di specifici procedimenti penali[10] (in casi di violenze sessuali, incesti, abusi su minori che diano luogo a gravidanze, traffico di minori) o su disposizione dell'autorità giudiziaria (nei casi, ad esempio, di abbandono di minore ove occorrano conferme per stabilire se sussistano i criteri di adottabilità, nei casi complessi di ricongiungimenti familiari di cittadini extracomunitari).

In alcune circostanze, seppur di rado, proprio per il fatto di essere ereditato e per la possibilità di ricostruire alberi genealogici e/o rapporti di parentela, il risultato di un'analisi genetica può fornire un vero e proprio impulso ed indirizzo alle indagini (basti pensare al caso dell'omicidio di Yara Gambirasio dove l'individuazione di Massimo Bossetti è avvenuta attraverso una complessa analisi massiva di profili genetici forniti su base volontaria e la ricostruzione di una serie di rapporti di parentela).

9 Si trattava di uno spazzolino da denti ed un tagliaunghie.

10 Non sono invece coinvolti nello svolgimento di test di paternità per dispute civili.

5. La genetica forense nell'ambito delle identificazioni di persone scomparse, cadaveri sconosciuti e vittime di disastri di massa

L'analisi dei 'polimorfismi del DNA autosomico nucleare', unitamente all'analisi delle impronte digitali ed all'analisi dell'arcata dentaria, rappresentano i tre approcci approvati dalla comunità scientifica internazionale a scopo identificativo.

I laboratori di genetica forense offrono supporto in tutti quei casi in cui si renda necessario verificare l'identità di una persona scomparsa, specialmente quando quest'ultima scompare nell'età dell'infanzia[11]. Inoltre, laddove si ipotizzi un sequestro di persona o comunque un fatto delittuoso, la ricerca di tracce biologiche all'interno di un'autovettura o di un appartamento può fornire elementi utili per le indagini.

Alla stregua di quanto detto fino ad ora, è comprensibile come si possa, attraverso l'analisi del DNA, identificare cadaveri sconosciuti e vittime di disastri di massa. In riferimento a quest'ultimo caso, con Decreto del Capo della Polizia del 06 aprile 2006, sulla scorta dell'esperienza maturata nell'identificazione delle vittime dello tsunami in Thailandia nel 2004 e dell'attentato terroristico a Sharm el Sheikh nel 2005, è stato istituito il 'Gruppo D.V.I.' (*Disaster Victim Identification*) della Polizia di Stato. Si tratta di una squadra multidisciplinare composta da medici legali, biologi, operatori di polizia scientifica, dattiloscopisti, interpreti e psicologi che interviene nei casi in cui ci siano delle vittime di un disastro di massa da identificare. Il Gruppo opera secondo i protocolli operativi messi a punto dall'Interpol che prevedono la raccolta dei dati *ante mortem*, ossia quelli relativi alla persona da identificare forniti da congiunti, e *post mortem*, ossia quelle informazioni che si riferiscono alla vittima a seguito del suo ritrovamento.

Nel caso degli accertamenti genetico-forensi, l'identificazione può essere diretta o indiretta: la prima consiste nel confronto tra il profilo genetico ottenuto da un campione prelevato dal cadavere da identificare e quello ottenuto da un effetto personale di uso certo ed esclusivo della persona; la seconda, invece, avviene attraverso l'effettuazione di un test di paternità o la costruzione di un albero genealogico

11 È il caso, ad esempio, delle piccole Angela Celentano e Denise Pipitone.

analizzando i campioni forniti dai prossimi congiunti per linea ascendente o discendente.

Dalla data della sua istituzione, il Gruppo D.V.I. della Polizia di Stato è intervenuto in diverse occasioni, tra le quali si ricordano la strage di Viareggio del 2009, il naufragio della Costa Concordia del 2012, il naufragio al largo di Lampedusa del 2013, la valanga di Rigopiano del 2017, l'incidente aereo in Etiopia del 2019 e il terremoto in Turchia del 2023.

6. La Banca Dati Nazionale del DNA

Nel mondo delle impronte digitali, la creazione dell'A.F.I.S. (*Automated Fingerprints Identification System*), ossia di un sistema di ricerca automatizzato per la ricerca di impronte digitali presenti in archivio, ha rappresentato una svolta epocale che, ancora oggi grazie allo zelante e necessario lavoro degli esperti dattiloscopisti, consente di attribuire impronte 'anonime' presenti sulla scena di un crimine a soggetti fotosegnalati.

Con il miglioramento e lo sviluppo delle tecniche per l'analisi dei polimorfismi genetici del DNA nucleare, è cresciuta la necessità di individuare un set di marcatori polimorfici[12] con alto potere discriminativo che possa essere utilizzato dai genetisti forensi in modo da poter rendere uniformi e comparabili i risultati ottenuti tra i diversi laboratori.

Sempre in Inghilterra, nel 1995, nasce la prima Banca Dati Nazionale del DNA, una raccolta di profili genetici costituita dall'insieme di quelli prelevati dalla scena di un crimine non attribuiti ad alcun soggetto e quelli delle persone per le quali la legge locale prevede l'obbligo dell'inserimento in Banca Dati.[13] La raccolta in un archivio informatizzato dei profili genetici di persone implicate in procedimenti penali permette la comparazione di questi con i profili genetici ottenuti dalle tracce biologiche rinvenute sulla scena di un crimine per poter risalire all'autore dello stesso. L'archivio genetico rappresenta una risorsa estremamente utile nei casi in cui le indagi-

12 Sequenze polimorfiche di DNA (presentano quindi più varianti alleliche) che si trovano in un locus (regione del DNA) specifico all'interno del cromosoma; si comportano in modo mendeliano e sono di facile rilevazione.

13 In Italia si fa riferimento all'art. 9 della L. n. 85/2009.

ni classiche non riescono a fornire un riscontro. L'inserimento dei profili 'anonimi' trovati sulla scena del crimine consente agli investigatori di collegare eventuali crimini seriali commessi dalla stessa persona.

Compresa l'importanza di tale potente ed efficace strumento investigativo, dopo l'Inghilterra, diversi paesi europei si sono dotati di una propria Banca Dati Nazionale del DNA le cui modalità di funzionamento e le cui regole nella gestione dei campioni di riferimento e permanenza dei profili all'interno dell'archivio, vengono gestiti secondo le rispettive leggi o regolamenti.

Nel 2005, il Trattato di Prum[14] impone a tutti i Paesi contraenti (tra cui l'Italia che recepirà il trattato solo nel 2009), l'istituzione di una Banca Dati Nazionale del DNA al fine di consentire gli scambi relativi al DNA dei condannati per reati commessi sui propri territori, di aumentare le misure di coordinamento nell'ambito delle indagini di polizia giudiziaria, di lavorare per la prevenzione di reati e coordinare la lotta al terrorismo transfrontaliero.

Con la legge del 30 giugno 2009, n. 85, vengono istituiti la Banca Dati Nazionale del DNA, cd. BDNDNA, ed il 'Laboratorio Centrale per la Banca Dati Nazionale del DNA'. Bisognerà, però, attendere il d.P.R. n. 87 del 7 aprile 2016[15] affinché la Banca Dati Nazionale del DNA diventi operativa.

Al fine di garantire una gestione delle informazioni relative a dati biologici in modo da tutelare il diritto alla privacy, il legislatore ha previsto che l'inserimento dei profili genetici anonimi ottenuti dall'analisi di tracce prelevate dalla scena di un crimine siano inseriti dai laboratori di genetica forense delle forze di polizia,[16] mentre l'inserimento dei profili genetici dei soggetti noti per i quali è previsto l'obbligo del prelievo di un campione biologico ai sensi dell'art. 9 della legge 85/2009, è a cura del Laboratorio Centrale del Dipartimento dell'Amministrazione Penitenziaria presso il carcere di Rebibbia. I laboratori di genetica forense e gli Istituti di Alta Specializzazione – purché accreditati ISO/IEC 17025 – presen-

14 Trattato sottoscritto da alcuni paesi membri dell'Unione Europea (Austria, Belgio, Francia, Germania, Lussemburgo, Spagna e Paesi Bassi) il 27 maggio 2005.

15 Regolamento recante disposizioni di attuazione della legge n. 85/2009.

16 Si fa riferimento ai laboratori accreditati ISO/IEC 17025.

ti sul territorio, possono alimentare la BDNDNA per il tramite del personale dei laboratori di genetica forense delle forze di polizia. In tutti i casi, l'inserimento di profili genetici all'interno della BDNDNA, è subordinata all'autorizzazione dell'Autorità Giudiziaria. Il software di gestione della BDNDNA italiana, così come nella maggior parte di paesi del mondo, è il 'CODIS' (*Combined DNA Index System*), ideato dall'FBI nel 1990.

Altra prerogativa della BDNDNA è quella di raccogliere i profili genetici delle persone scomparse e loro consanguinei al fine di identificare cadaveri sconosciuti o ancora di gestire l'identificazione di vittime di disastri di massa attraverso il modulo applicativo D.V.I.

Sebbene svariate banche dati del DNA contengano moltissimi dati, nessun Paese ha previsto l'inserimento dei profili genetici di una intera popolazione; ciò significa che, anche se venisse estrapolato un profilo genetico da una traccia presente sulla scena di un crimine, a meno che il profilo genetico dell'autore del reato non sia già inserito nel 'database', non sarebbe possibile ottenere un riscontro.[17] Tuttavia, i profili genetici inseriti all'interno della banca dati rimangono in costante modalità di ricerca. Per ulteriori informazioni riguardo la gestione della BDNDNA, si rimanda ai contenuti della legge n. 85 del 2009 e del d.P.R. n. 87 del 2016.

7. Gruppi di lavoro

L'impatto della genetica forense nelle indagini di polizia giudiziaria e l'interesse della comunità scientifica per questa scienza hanno reso necessaria l'istituzione di gruppi di lavoro in ambito internazionale e nazionale.

I genetisti forensi della Polizia Scientifica partecipano attivamente al Gruppo di lavoro E.N.F.S.I. DNA – WG (*ENFSI DNA Working Group*). L'E.N.F.S.I. (*European Network of Forensic Science Institutes*), fondato nel 1995, è un network europeo di istituti di scienze forensi – oggi allargato almeno per la genetica forense anche all'FBI ed a paesi extra europei – nato con lo scopo di facilitare lo scambio di informazioni nel campo delle scienze forensi, produrre linee guida, diffondere

17 Il cosiddetto *match*.

raccomandazioni, predisporre manuali, oltre che guidare la comunità scientifica verso obiettivi comuni e sviluppare progetti per migliorare il potere informativo dei risultati basati sull'analisi del DNA.

In ambito nazionale, sempre al fine di condividere conoscenze e promuovere l'armonizzazione e l'adozione di metodiche analitiche adeguate attraverso la produzione di linee guida e raccomandazioni, la Polizia Scientifica partecipa ai lavori del 'Gruppo Ge.F.I.' (Genetisti Forensi Italiani), gruppo di lavoro di lingua italiana dell'ISFG (*International Society for Forensic Genetics*) nato nel 1975.

Alla luce di progressi degli ultimi vent'anni, la genetica forense risulta uno strumento molto utile nel fornire un contributo per casi rimasti insoluti. Con l'avvento e lo sviluppo di tecnologie sempre più sensibili in grado di fornire profili genetici anche da tracce esigue di DNA, è aumentata la possibilità di poter riaprire casi, lontani nel tempo, per i quali non erano stati analizzati i reperti o, magari, pur essendo stati analizzati le tecniche del momento non consentivano di fornire profili genetici con alto potere discriminativo.

Con Decreto del Capo della Polizia del 3 agosto 2009, viene istituita, presso la Direzione Centrale Anticrimine del Dipartimento della Pubblica Sicurezza, l'U.D.I. (Unità Delitti Insoluti): si tratta di un gruppo, composto da personale investigativo dello S.C.O. (Servizio Centrale Operativo) e del Servizio Polizia Scientifica, per lo svolgimento di attività tecniche nei vari settori delle scienze forensi, al quale è assegnato il compito di analizzare e coordinare le indagini avviate su casi criminali accaduti in passato e non ancora risolti.

8. Considerazioni finali e prospettive future

Dopo 120 anni di storia, quello che emerge è l'immutabilità dei principi che stanno alla base dell'analisi di un'impronta digitale, così come analoghi alle loro origini sono i criteri e l'approccio utilizzati per l'analisi della scena di un crimine. Non è però da trascurare il fatto che le innovazioni tecnologiche e la produzione di apparecchiature e strumenti – si pensi ad esempio alla fotografia, alle fonti di luce, all'ottica per gli ingrandimenti

ed alla digitalizzazione – abbia notevolmente migliorato il risultato finale rispetto a quanto avveniva in origine.

La genetica forense, invece, si può considerare una scienza applicata al diritto estremamente 'giovane', soprattutto se paragonata agli strumenti tipicamente riconducibili alla scuola di Ottolenghi quali la dattiloscopia e gli altri metodi rigorosi messi a punto per l'analisi di una scena del crimine e per la cristallizzazione dello stato dei luoghi. Nonostante la storia recente della genetica forense, le innovazioni tecnologiche cui abbiamo assistito in questi ultimi quarant'anni appaiono delle vere e proprie rivoluzioni copernicane. In questo arco temporale, infatti, è cambiato l'approccio metodologico e analitico e vengono proposti nuovi marcatori, nuovi software di analisi, apparecchiature e kit sempre più performanti. Tutto questo, se da una parte consente ai genetisti forensi di ottenere risultati anche da tracce estremamente esigue e/o degradate, dall'altra, soprattutto quando di parla di DNA da contatto (*touch* DNA), rende necessario da parte dello scienziato forense l'uso di una particolare cautela e prudenza nella presentazione dei risultati al fine di non fare incorrere i non addetti ai lavori in incomprensioni che potrebbero generare errori giudiziari.

Il genetista forense è oggi chiamato a rispondere a domande quali: da quale fonte proviene il DNA trovato sulla scena di un crimine? Come è arrivato sulla scena o su un reperto? La comunità scientifica ha avviato progetti di ricerca e sperimentazioni in più laboratori nel mondo per comprendere quali possano essere i limiti o le potenzialità di un risultato ottenuto da tracce esigue di DNA da contatto.

Il costante sviluppo delle tecniche analitiche consente, oggi, di poter utilizzare marcatori genetici in grado di indagare i cosiddetti tratti fenotipici quali il colore dei capelli, degli occhi, l'età anagrafica ed il gruppo popolazionistico di appartenenza. Tale approccio non può trovare ancora spazio nella routine dei laboratori di genetica forense delle forze di polizia poiché risulta ancora essere molto costoso e con risultati che si esprimono in termini percentuali che, in alcuni casi, potrebbero risultare fuorvianti per le indagini.

L'approccio basato sull'impiego di questi nuovi sistemi è pensato, come ulteriore risorsa, per quei casi di particolare gravità dove non vi sono sviluppi investigativi o spunti di in-

teresse con le indagini classiche. Proprio perché la genetica forense è una scienza in continua evoluzione, quelle che oggi vengono definite come 'nuove frontiere', domani potranno essere parte integrante delle analisi di routine, se non addirittura essere soppiantate da altre metodiche più informative e performanti.

Per concludere, sebbene l'analisi del DNA in campo forense possa essere considerata un elemento imprescindibile nelle indagini di polizia giudiziaria ed abbia consentito di risolvere tanti casi giudiziari, non bisogna perdere di vista che la stessa rappresenta soltanto uno dei tasselli da inserire nell'insieme degli elementi circostanziali del caso. Non può essere, salvo in rari casi, l'unico elemento fondante di un'indagine.

Come disse Jules Henri Poincarè ne "La scienza e l'ipotesi", la scienza si costruisce con i fatti come una casa con le pietre. Ma una collezione di fatti non è una scienza, più di quanto un mucchio di pietre non sia una casa.

LA PROVA DEL DNA NEL PROCEDIMENTO PENALE

Luisa Bettiol
Procura della Repubblica presso il Tribunale di Palermo

Abstract: DNA evidence is an evidence marked by high technicality and in constant evolution both in genetics laboratories and in courtrooms. It is decisive evidence in cases of serious crimes against sexuality in which it often happens that the perpetrator leaves biological traces at the crime scene or on the victim's body.

Parole chiave: indagini genetiche; DNA; processo penale.

1. Premessa

Nel procedimento penale si definisce 'prova scientifica' la "prova che, partendo da un fatto dimostrato, utilizza una legge scientifica per accertare l'esistenza di un ulteriore fatto da provare".[1]
Tale è la prova del DNA in cui l'indagine genetica mira all'attribuzione di una traccia biologica ad un dato individuo sulla base di un calcolo probabilistico rigoroso.[2]

Si tratta di un tipo di investigazione che ha assunto nel corso degli anni un ruolo cruciale nell'accertamento dei fatti di reato.

Sempre più spesso accade che l'esperimento di accertamenti genetici si riveli decisivo per la prova della colpevolezza dell'imputato, in presenza di un quadro probatorio altrimenti meramente indiziario ovvero in assenza di adeguati elementi di riscontro.

Per richiamare le parole del celebre criminologo francese Edmond Locard "ogni contatto lascia una traccia".[3] Ecco che il rinvenimento del DNA di un soggetto in un certo luo-

1 Tonini 2003: 1459 ss.

2 Presciuttini 2019.

3 Si tratta di un aforisma semplificato derivante dalla citazione originale: "La verità è che nessuno può agire con l'intensità propria delle attività criminali senza lasciare tracce multiple del suo passare. ... gli indizi di cui io voglio parlare sono di due generi: qualche volta il criminale lascia le tracce su una

go dimostra il fatto che questi vi è stato presente lasciando parte del proprio materiale biologico. Tale dato, in assenza di una spiegazione alternativa plausibile, può offrire la dimostrazione del collegamento tra l'autore ed il fatto delittuoso. Così, nel caso di gravi reati contro la persona quali omicidi, maltrattamenti e violenze sessuali, la prova biologica del reo viene di frequente rinvenuta sul corpo della vittima e risulta molto spesso decisiva nel desumere la colpevolezza di un dato soggetto.

La portata straordinaria di una simile prova, nonché la sua formazione secondo leggi scientifiche, impongono particolari cautele nella raccolta delle tracce biologiche, nella conservazione e nella successiva fase di analisi. Al contempo, tale tipologia di accertamento pone l'esigenza di coniugare i connotati tipici del mondo scientifico – a fronte di una prova, quella del DNA, 'esplicitamente probabilistica'[4] – con l'ambito processuale, in cui il giudice chiede alla scienza risposte quanto più possibile chiare ed univoche, secondo il canone 'al di là del ragionevole dubbio'.

2. La natura dell'indagine genetica

Il ricorso all'indagine genetica può risultare fondamentale per attribuire un'identità all'autore del delitto in tutti i casi in cui sulla scena del crimine, o sulle cose utilizzate dal reo successivamente repertate, siano rinvenibili tracce biologiche appartenenti al medesimo – quali ad esempio saliva, sangue, liquido seminale, tracce da contatto o sudore – dalle quali sia possibile ricavare un profilo genetico.

Una simile prova può essere legittimamente utilizzata dal giudice per fondare un giudizio di colpevolezza ovvero di innocenza di un determinato soggetto.

Per le indagini di genetica forense risulta necessario procedere alla elaborazione di un resoconto dettagliato di quanto accaduto alla vittima, con particolare riguardo a diversi profili: l'epoca in cui è avvenuto il fatto, il numero degli ag-

scena con le sue azioni; altre volte, raccoglie sui suoi vestiti o sul suo corpo tracce dei suoi movimenti e della sua presenza", Locard 1920.

4 Presciuttini 2019: XI.

gressori, la tipologia di contatto fisico, l'indicazione di eventuali precedenti rapporti consenzienti con l'aggressore ed il relativo periodo di riferimento, ed infine ogni attività svolta dalla vittima nel momento successivo[5] alla violenza. Così, le lesioni eventualmente presenti sul corpo della vittima di violenza possono fornire prove preziose ed essere sede di tracce biologiche dell'aggressore.[6]

Secondo la giurisprudenza della Corte di cassazione "in tema di prove, gli esiti dell'indagine genetica condotta sul DNA hanno natura di prova piena e non di mero elemento indiziario, atteso l'elevatissimo numero delle ricorrenze statistiche confermative, tale da rendere infinitesimale la possibilità di un errore, sicché sulla loro base può essere affermata la penale responsabilità dell'imputato, senza necessità di ulteriori elementi convergenti" (cfr., da ultimo, Cass., Sez. II, 6 luglio 2022, n. 38184).[7] In tale pronuncia, la Suprema Corte – richiamando un orientamento ormai consolidato – ha ribadito con riguardo a detti esiti che "presentano natura di prova e non di mero elemento indiziario ai sensi dell'art. 192, comma secondo, c.p.p.; peraltro, nei casi in cui l'indagine genetica non dia risultati assolutamente certi, ai suoi esiti può essere attribuita valenza indiziaria (Sez. II, 5 febbraio 2013, n. 8434, Mariller, Rv. 25527; Sez. I, 30 giugno 2004, n. 48349, Rizzetto, Rv. 231184)".

Per compiere un simile accertamento, connotato da un elevato tasso di tecnicismo, il pubblico ministero nel corso delle indagini, il giudice e le parti private devono necessariamente affidarsi all'opera di specialisti ed essere così supportati dall'indispensabile contributo degli esperti, come il personale di Polizia Scientifica.

5 Ad esempio, se la stessa si sia cambiata gli indumenti, se dovesse essersi lavata ed altre eventuali informazioni a riguardo.

6 Per un approfondimento in dottrina Buscemi, Barni 2021: 1063 ss.

7 In questo senso si veda, *ex plurimis*, anche Cass., Sez. II, 1 giugno 2016 (dep. 13 ottobre 2016), n. 43406, Syziu: "Gli esiti dell'indagine genetica condotta sul DNA hanno natura di prova, e non di mero elemento indiziario ai sensi dell'art. 192, comma secondo, cod. proc. pen, sicché sulla loro base può essere affermata la responsabilità penale dell'imputato, senza necessità di ulteriori elementi convergenti".

Al riguardo la Suprema Corte[8] ha indicato la necessità per gli operatori del diritto di approcciarsi alla prova del DNA avendo consapevolezza e padronanza del lessico che ne è proprio e che si sviluppa a partire dal concetto di probabilità. In particolare, i giudici di legittimità hanno ricostruito il quesito dal quale muovono le indagini genetiche, ossia stabilire quanti sono gli individui nella popolazione rilevante per il caso di specie che possiedano lo stesso profilo genetico. In altri termini, affermare la compatibilità genetica di due profili equivale a pronunciarsi sulla probabilità che un determinato soggetto possegga un profilo genetico corrispondente a quello estratto dalle tracce biologiche repertate sui luoghi e a seguito della commissione del reato.

Occorre poi rilevare come la prova del DNA possa venire in rilievo non soltanto per fondare un giudizio di colpevolezza quanto anche per dimostrare un fatto secondario – ad esempio il contatto con un oggetto o un rapporto di conoscenza tra la vittima e il sospettato – ovvero anche per fornire dati utili per le indagini, disporne di ulteriori, sostenere o contraddire le dichiarazioni delle parti coinvolte.

Allo stesso tempo, il DNA esprime le sue potenzialità sul versante della dimostrazione dell'innocenza di un determinato soggetto, in caso di mancata corrispondenza dei tratti identificativi dei due profili genetici analizzati. Proprio in ragione del risultato di esclusione, come nei casi di reati di violenza sessuale, l'evidenza genetica viene considerata come la 'regina delle prove a discarico'.

3. La formazione della prova del DNA

Nel procedimento probatorio in materia genetica si possono individuare tre fasi operative conseguenziali e propedeutiche: l'individuazione e la raccolta del reperto biologico, l'invio al personale di Polizia Scientifica per gli accertamenti tecnici volti all'estrazione del DNA e l'attività di comparazione.[9]

8 Cfr. Cass., Sez. I, 12 ottobre 2018, n. 52872 con nota a sentenza, tra i molti, di Gigli 2019: 2537.

9 Sul tema si veda Parodi 2022: 80 ss.; Buscemi, Barni: 26 ss.

La cd. repertazione costituisce la prima fase di acquisizione della traccia biologica. Essa avviene nel corso di appositi sopralluoghi compiuti dal personale di polizia giudiziaria sulla scena del crimine e comporta il sequestro del materiale ritenuto di interesse investigativo.

A tale attività segue l'inoltro del reperto acquisito agli esperti di indagini scientifiche, i quali sono chiamati alla tipizzazione genetica della traccia. In caso di esito positivo, viene realizzata l'attività che racchiude il principale obiettivo dell'intera indagine di biologica e genetica forense: l'identificazione del donatore della traccia.

L'attribuzione di una traccia biologica ad un determinato individuo può avvenire in via cd. diretta, attraverso la comparazione con il profilo genetico di confronto di un soggetto di interesse a cui è stato prelevato nel corso delle indagini, ovvero in via cd. indiretta, ricorrendo alla Banca Dati Nazionale del DNA.[10] Nel caso preso per ultimo in considerazione, la comparazione avviene con milioni di altri profili di DNA archiviati e ciò al fine di ricercare un riscontro completo, o anche solo parziale, in grado di condurre all'identificazione di un parente di quell'individuo.[11]

Si rileva, con riguardo a quest'ultimo profilo, che i più recenti sviluppi nell'analisi del DNA nucleare hanno portato ad elaborare modelli predittivi di caratteristiche somatiche dell'individuo che vengono ricostruite in laboratorio secondo varie incidenze statistiche, analizzando specifiche componenti del DNA.

Come sottolineato anche dalla Suprema Corte nella sentenza 12 ottobre 2018, dep. 23 novembre 2018, 52872 (imp. Bossetti), "i *predictive DNA markers* consentono, cioè, di individuare alcuni caratteri esterni dell'individuo di cui non si conosca l'identità anagrafica, quali il colore degli occhi e il colore dei capelli. È, dunque, possibile individuare, allo stato attuale dello sviluppo della metodica, due caratteri fenotipici in grado di restringere il campo dei sospettati".

L'*iter* che ha condotto all'attuale disciplina della Banca Dati Nazionale del DNA prende le mosse dalle disposizioni contenute nel Trattato di Prüm, concluso il 27 maggio 2005

10 Sul tema, tra gli altri, si vedano Rivello 2016: 1521 ss.; Biondo 2016: 214 ss.

11 Cfr. Presciuttini 2019: XII.

ed entrato in vigore il 1° novembre 2006, volto a rafforzare la cooperazione tra gli Stati nella lotta contro il terrorismo, la criminalità transfrontaliera e l'immigrazione illegale,[12] a cui è stata data completa attuazione nel nostro Paese a partire dal 2015.[13]

Una delle principali funzioni della banca dati consiste nel confrontare costantemente i profili del DNA provenienti dai reperti biologici rinvenuti sulla scena del crimine con quelli dei soggetti sottoposti a prelievo in occasione di precedenti controlli o arresti.[14]

Il confronto tra il genotipo estrapolato dal reperto ed il genotipo di riferimento può dare origine, nella pratica operativa, a tre diversi esiti: concordanza / compatibilità genetica, discordanza / incompatibilità e inconclusività.

Tale ultimo risultato descrive la situazione in cui, dal confronto del profilo genetico del reperto con quello di un campione di confronto, non è possibile trarre, a seguito di una valutazione probabilistica, un giudizio di inclusione ovvero di esclusione; ciò può conseguire a diversi aspetti problematici, come ad esempio profili genetici incompleti o parziali, una

12 Tale trattato è stato stipulato originariamente tra la Repubblica austriaca, il Regno del Belgio, la Repubblica francese, la Repubblica federale di Germania, il Granducato del Lussemburgo, il Regno dei Paesi Bassi e il Regno di Spagna; l'Italia ha aderito alcuni anni dopo.

13 Rif. decreto 8 novembre 2016 "Procedure per il trattamento dei dati, da parte della banca dati del DNA e del laboratorio centrale per la banca dati nazionale del DNA, e per la trasmissione del profilo del DNA da parte dei laboratori di istituzioni di elevata specializzazione, in attuazione degli articoli 3, 4 e 6 del decreto del Presidente della Repubblica 7 aprile 2016, n. 87", Gazzetta Ufficiale, 2016, n. 296. Lo schema di decreto del Presidente della Repubblica, concernente il Regolamento recante disposizioni di attuazione della legge 30 giugno 2009 n. 85, sull'istituzione della banca dati nazionale del DNA e del laboratorio centrale per la banca dati nazionale del DNA – in attuazione dell'articolo 16, comma 1, l. n. 85 del 2009 – è stato approvato in via preliminare dal Consiglio dei ministri soltanto il 3 luglio 2015.

14 Al fine di operare il raffronto automatizzato dei profili del DNA, il software della Banca dati è organizzato su due livelli. Il primo livello, ai sensi dell'art. 3, comma 4, del Regolamento è utilizzato ai fini investigativi in ambito nazionale; invece, il secondo livello viene impiegato, in conformità alle Decisioni 2008/615 GAI e 2008/616/GAI, e successive modificazioni, anche per le finalità di collaborazione internazionale di polizia, ai sensi dell'art. 12 della L. n. 85 del 2009.

quantità limitata di DNA estratto, la degradazione del materiale biologico o l'intervento di fattori contaminanti.[15]

Laddove la comparazione tra un profilo genetico di un reperto biologico ed un profilo genetico di un campione biologico mostrino una concordanza o una compatibilità tali da inferire il contributo genetico di quel soggetto alla genesi della traccia sul reperto oggetto di indagine è opportuno procedere a ponderare, con una valutazione probabilistica, quanto tale concordanza o compatibilità biologica corrisponda ad una effettiva identificazione del soggetto o dei soggetti di interesse.

Come rilevato dalla Suprema Corte nella citata sentenza del 12 ottobre 2018, n. 52872, quanto alla capacità identificativa dell'analisi del DNA,

> nell'ottica del confronto uno a uno tra campioni, la comunità scientifica afferma che la sovrapposizione del profilo genetico individuato in una traccia su quello oggetto del confronto può essere completa o non completa.
> Per la validazione del risultato vengono in rilievo l'adozione di metodologie analitiche accettate dalla comunità scientifica e il rispetto degli standard garantito dalla certificazione e dall'accreditamento dei laboratori, ormai obbligatorie ai sensi della legge istitutiva della Banca nazionale del DNA.

Sovente nella prassi si pongono, altresì, casi di commistioni biologiche che pongono particolari criticità nell'analisi, dapprima per il genetista forense e poi, nel corso della valutazione della prova, per l'organo giudiziario. Così, ad esempio, nei casi di violenza sessuale di gruppo, ciascun aggressore può contribuire con proporzioni differenti del proprio materiale genetico alla formazione della traccia biologica oggetto di analisi. Occorrerà quindi valutare il numero dei soggetti contributori, la proporzione del DNA dei diversi soggetti e le condizioni di integrità differenziale del DNA degli stessi.

In concreto, il prelievo del campione biologico da comparare può avvenire con il consenso del soggetto, in via coattiva ovvero all'insaputa dello stesso.

15 V. Previderè, Fattorini 2016: 179 ss.

Con riguardo alla prima eventualità, la giurisprudenza di legittimità è consolidata nel ritenere che il prelievo genetico effettuato con il consenso da parte dell'indagato può avvenire "anche in assenza del difensore, ciò in ragione della specifica e limitata finalità dell'atto di prelievo, che non implica speciali competenze tecniche comportanti l'esigenza di osservare precise garanzie difensive, necessarie invece per la successiva attività di valutazione dei risultati" (cfr. Cass., Sez. III, 1 luglio 2015, 25426; Cass., Sez. V, 7 febbraio 2017, n. 12800).

Laddove non sia prestato il consenso, è possibile procedere al prelievo coattivo di materiale biologico, disciplinato dal legislatore agli artt. 224-*bis* e 359-*bis* c.p.p. secondo uno schema in grado di conciliare le esigenze di tutela della libertà personale dell'individuo con quelle di accertamento del reato. Sul punto, l'inosservanza di una serie di disposizioni in tema di assistenza difensiva, avvisi, accompagnamento coattivo e modalità delle operazioni può comportare l'inutilizzabilità degli esiti.[16]

Quanto alla terza eventualità, la Suprema Corte ha ritenuto legittima l'attività di raccolta di tracce biologiche riferibili all'indagato eseguita dalla polizia giudiziaria senza ricorrere ad alcun prelievo coattivo ancorché attuata all'insaputa dello stesso. Un simile accertamento può rispondere ad esigenze di segretezza delle indagini ovvero trovare ragione nel fatto che non vi sia ancora contezza dell'identità del possibile autore.

L'acquisizione può avvenire anche con *screening* di massa, nei casi in cui si mira a determinare il profilo genetico di tutte indistintamente le persone che appartengono ad una data categoria o insieme – ad esempio perché abitanti in un una determinata area geografica in ipotesi dove è avvenuto il delitto –, e si ha motivo di ritenere sulla base delle investigazioni condotte che l'autore del reato appartenga al già menzionato insieme. Tale tecnica è utile anche per individuare la cerchia familiare a cui appartiene l'ignoto autore, e così giungere più agevolmente all'individuazione del reo.

La giurisprudenza si è pronunciata in più occasioni in termini di legittimità dell'attività di prelievo all'insaputa del sospettato. In particolare, con riguardo all'acquisizione di campione salivare residuo – dopo l'uso dell'etilometro – sul

16 Per un approfondimento si veda Parodi 2022: 82 ss.

boccaglio dell'apparecchio di misurazione la Suprema Corte ha sottolineato che

> può essere effettuato ai sensi dell'art. 348 c.p.p., in quanto l'attività non determina alcuna incidenza sulla sfera della libertà personale dell'interessato, riguardando materiale biologico fisicamente separato dalla persona (*ex multis*: Cass., Sez. II, 7 ottobre 2016, n. 51086, Franchin, Rv. 269223; in precedenza Sez. I, 2 novembre 2005 (dep. 2006), n. 1028, Esposito ed altro, Rv. 233132).

È manifestamente infondata e perciò inammissibile la denuncia di violazione dell'art. 114 disp. att. c.p.p., poiché l'avviso ivi previsto è dovuto soltanto quando si procede agli atti di cui all'art. 356 c.p.p. (perquisizioni *ex* art. 352 c.p.p.; accertamenti urgenti e sequestro *ex* art. 354 c.p.p.; immediata apertura della corrispondenza a norma dell'art. 353 comma 2 c.p.p.) tra cui non rientra l'acquisizione *ex* art. 348 c.p.p. del boccaglio abbandonato né, tanto meno, le successive attività di estrazione del DNA in quanto ripetibili.[17]

4. La valutazione dell'indagine genetica nel processo penale

Nel corso del processo il giudice che deve confrontarsi con la prova del DNA è chiamato a valutarne la validità e l'attendibilità.

Ancor prima che l'organo giudicante possa esercitare il suo libero convincimento sul valore probatorio da attribui-

17 Rif. Cass., Sez. I, 12 ottobre 2018, dep. 23 novembre 2018, n. 52872, Bossetti. Così, il prelievo di saliva, avvenuto all'insaputa dell'imputato, mediante il sequestro di un bicchierino di caffè offerto dalla polizia giudiziaria, può essere effettuato ai sensi dell'art. 348 c.p.p. in quanto l'attività non determina alcuna incidenza sulla sfera della libertà personale dell'interessato, riguardando materiale biologico fisicamente separato dalla persona (cfr. Cass., Sez. I, 2 novembre 2005, n. 1028); allo stesso modo, per il prelievo di saliva, avvenuto all'insaputa dell'imputato, su mozziconi di sigaretta ed un *cotton fioc* v. Cass., Sez. II, 7 ottobre 2016, n. 51086; così, Cass., Sez. I, 20 novembre 2013, n. 48907, ha ritenuto legittimo il prelievo di tracce biologiche da un mozzicone di sigaretta maneggiata e fumata dall'indagato, acquisito dalla polizia giudiziaria dopo che l'indagato medesimo l'aveva abbandonato, pur sottolineando le necessarie garanzie sulla provenienza dello stesso.

re all'indagine genetica, occorre controllare la regolarità del percorso che ha portato alla sua formazione sia dal punto di vista giuridico sia quanto a potenziali inquinamenti o contaminazioni idonei a minare in radice la possibilità di un'analisi affidabile da parte dello scienziato.[18]

Spesso nelle aule giudiziarie viene invocata dalle parti del processo la violazione di norme procedurali ovvero cautelari, previste da protocolli o linee guida – delle più svariate provenienze – per farne derivare, più o meno direttamente, l'inutilizzabilità probatoria dei risultati aggiunti degli esiti ovvero l'inaffidabilità delle valutazioni proposte dall'esperto.[19]

Così, quanto al primo profilo, la Suprema Corte è intervenuta in più occasioni a chiarire quali accertamenti genetici debbono essere perfezionati inderogabilmente seguendo l'art. 360 c.p.p., dalla cui violazione discende la possibile nullità dell'atto compiuto e la conseguente inutilizzabilità dei relativi esiti.

In particolare, la Suprema Corte distingue la raccolta o il prelievo dei dati pertinenti al reato, dall'accertamento tecnico irripetibile, che riguarda, invece, il loro studio e la loro valutazione critica (cfr. Cass., Sez. VI, 6 febbraio 2013, n. 10350; Cass., Sez. II, 10 gennaio 2012, n. 2087; Cass., Sez. II, 10 luglio 2009, n. 34149; Cass., Sez. I, 31 gennaio 2007, n. 14852).

Come detto, il rilievo tecnico consiste nell'attività di raccolta di elementi attinenti al reato per il quale si procede, mentre l'accertamento tecnico, ripetibile o irripetibile, si estende al loro studio e alla loro valutazione critica secondo canoni tecnici o scientifici.[20]

18 Cfr. Lupària 2016: 170 ss.; sul tema si veda anche Taroni *et al*.: 15 ss.

19 Il riferimento a 'protocolli' è qui per indicare un complesso di regole e procedure che, in un determinato ambito o disciplina (come, ad esempio, nel campo della medicina), devono essere osservate per la corretta esecuzione di una determinata attività. In tal senso si possono richiamare le raccomandazioni adottate dall'E.N.F.S.I. (*European Network Forensic Science Institutes*, istituto scientifico europeo di riferimento in ambito scientifico-forense, al quale aderiscono molti tra i più autorevoli enti scientifici nazionali), le quali assumono di regola la denominazione di '*guidelines*', '*recommendations*' o '*best practices*'. Così pure, restando all'interno dei confini nazionali in ambito genetico, sono denominate 'raccomandazioni' quelle recentemente adottate dai Genetisti forensi italiani (GEFI), nel gennaio 2018 oppure 'criteri minimi' le linee guida adottate dalla Società italiana di genetica umana (SIGU) nel dicembre 2016.

20 Cfr. Cass., Sez. II, 10 luglio 2009, n. 34149.

I prelievi sul DNA, attraverso il sequestro di oggetti contenenti tracce organiche di interesse, qualificabili come rilievi tecnici delegabili *ex* art. 370 c.p.p., non sono atti invasivi o costrittivi, essendo solo prodromici allo svolgimento di successivi accertamenti tecnici e non richiedono in quanto tali l'osservanza di garanzia difensive.[21]

In senso conforme si è espressa la Corte costituzionale nella sentenza 26 settembre 2017, n. 239 che ha rigettato la questione di legittimità costituzionale dell'art. 360 c.p.p. "ove non prevede che le garanzie difensive previste da detta norma riguardano anche le attività di individuazione e prelievo di reperti utili per la ricerca del DNA" sollevate in riferimento agli articoli 24 e 11 della Costituzione.

Nel corso delle argomentazioni, la Consulta ha rilevato che

> Il solo fatto che concerna rilievi o prelevamenti di reperti "utili per la ricerca del DNA" non modifica la natura dell'atto di indagine e non ne giustifica di per sé la sottoposizione a un regime complesso come quello previsto dall'art. 360 c.p.p., costituito dalla nomina di un consulente, dall'avviso all'indagato, alla persona offesa e ai difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico, dalla possibilità per l'indagato di promuovere un incidente probatorio, con il divieto per il pubblico ministero di procedere agli accertamenti (e, secondo la richiesta estensione della norma, anche ai rilievi e ai prelevamenti in questione) salvo che questi, se differiti, non possano più essere utilmente compiuti.
>
> Ad esempio, il prelievo di capelli o di peli rinvenuti in posti sotto l'aspetto probatorio significativi non si differenzia dal prelevamento di altri reperti e non ci sarebbe ragione di effettuarlo con le forme previste dall'art. 360 c.p.p. ...
>
> Neppure al prelievo di tracce biologiche si potrebbero di regola riconoscere caratteristiche tali da differenziarlo da qualunque altra operazione di repertazione. Senza considerare che l'esistenza – alla quale ha fatto riferimento il giudice rimettente – di protocolli per la ri-

21 Cfr. Cass., Sez. I, 2 febbraio 2005, n. 8393.

> cerca e il prelievo di tracce di materiale biologico può, da un lato, rendere routinaria l'operazione e, dall'altro, consentirne il controllo attraverso l'esame critico della prescritta documentazione.
> E non è privo di rilevanza che nel dibattimento l'imputato abbia la possibilità di verificare e contestare la correttezza dell'operazione anche attraverso l'esame del personale che l'ha eseguita, oltre che dei consulenti tecnici e dell'eventuale perito nominato dal giudice.
> È da aggiungere che le forme dell'art. 360 c.p.p. potrebbero assai spesso risultare incompatibili con l'urgenza, nel corso delle indagini, di eseguire il prelievo.

Diverso è il procedimento volto all'identificazione del DNA della persona attraverso i campioni di materiale genetico repertati, le cui attività saranno qualificabili come ripetibili o irripetibili a seconda che, sulla base di una valutazione di natura solo tecnico-fattuale, comportino la distruzione o il grave deterioramento dei campioni utilizzati.

Come detto, l'attribuzione di una traccia biologica ad un dato individuo si articola in tre fasi distinte, ossia nell'estrapolazione del profilo genetico presente sui reperti, nella decodificazione dell'impronta genetica dell'indagato e nella comparazione tra i due profili. Delle tre operazioni possono rinvenirsi profili di irripetibilità sono nella prima e possono derivare sia dalla scarsa quantità della traccia genetica sia dalla scadente qualità del DNA presente nella stessa.[22]

Infine, i risultati del procedimento attraverso il quale si giunge all'identificazione del DNA della persona vengono trasposti in supporti documentali nei quali è riversata la composizione della catena genomica rilevata dall'analisi dei campioni di materiale genetico. Tali dati sono stabili e non modificabili, con la conseguenza che la comparazione genetica si risolve nel confronto dei supporti documentali su cui sono stati registrati i profili genotipici estratti attraverso l'attività tecnica. Pertanto, la comparazione costituisce un'operazione sempre ripetibile, a condizione che sia assicurata la

22 Cfr. Cass., Sez. II, 27 novembre 2014, n. 2476.

corretta conservazione dei supporti sui quali sono impresse le impronte genetiche.[23]

Ne consegue che la natura irripetibile dell'accertamento tecnico e la necessaria osservanza della disciplina dell'art. 360 c.p.p. deve essere accertata in concreto, dipendendo dalla quantità della traccia e dalla qualità del DNA sulla stessa presente.

In ogni caso, rimane ferma l'utilizzabilità degli esiti degli accertamenti tecnici irripetibili compiuti senza le garanzie previste dall'art. 360 c.p.p. – se non nei confronti della parte offesa dal reato – se all'epoca si procedeva contro ignoti ovvero contro un soggetto diverso da quello successivamente indagato, non essendo ancora stato identificato il soggetto poi individuato quale autore del reato.[24] Così, più in generale, la Suprema Corte ha affermato: "In tema di accertamento tecnico non ripetibile, gli avvisi di cui all'art. 360, comma 1, c.p.p., sono dovuti solo in presenza di consistenti sospetti di reato, sia sotto il profilo oggettivo che in ordine alla sua attribuibilità" (rif. Cass., Sez. IV, 28 gennaio 2021, n. 20093).

Ulteriori problematiche nell'analisi della validità e dell'affidabilità degli esiti della prova genetica possono poi conseguire all'inosservanza delle regole procedurali prescritte dai protocolli scientifici internazionali o dalle linee guida.

Sul punto, la dottrina e giurisprudenza maggioritarie ritengono che non ogni violazione dei protocolli determini la formazione di un risultato viziato. La sanzione, in caso di ritenuta violazione dei 'protocolli' relativi all'espletamento di indagini genetiche (sia essa intervenuta nella fase di repertamento delle tracce biologiche o in quella successiva di conservazione delle tracce repertate o, infine, in quella analitica vera e propria) può essere l'attenuata valenza dimostrativa del risultato di prova, se non addirittura la inutilizzabilità della prova stessa, non già quale conseguenza automatica della violazione dei protocolli, bensì della inaffidabilità ritenuta dal giudice a seguito dell'esame della concreta incidenza della violazione nel caso specifico.[25]

23 Cfr. Cass., Sez. I, 12 ottobre 2018, n. 52872, cit; in senso conforme anche Cass., Sez. II, 30 maggio 2019, n. 41414.

24 Cfr. Cass., Sez. I, 12 ottobre 2018, n. 52872, cit.

25 Sulla tematica, si veda in dottrina Valli 2018: 15 e ss.; Felicioni 2018: 1620 ss.

Un caso emblematico sul punto è rappresentato dalla richiesta di revisione del processo Stasi avanzata nel dicembre 2016, mediante deposito di memoria presso la Procura Generale della Corte d'appello di Milano, nella quale si chiedeva – tra le altre cose – di rivalutare gli esiti della perizia genetica eseguita nel corso del processo di merito (anche) sui margini ungueali di Chiara Poggi. Il risultato raggiunto dal perito aveva permesso di identificare, a fianco del DNA della vittima (nettamente preponderante) la presenza di un DNA maschile (attraverso l'analisi dei marcatori siti sul cromosoma Y) e non anche di attribuire detto DNA all'imputato o a terzi. Tuttavia, nel caso di specie, il perito risultava essersi discostato dalle norme tecniche dettate dalle linee guida elaborate dalla comunità scientifica di riferimento e per questo è stato messo in dubbio l'attendibilità dei relativi esiti.[26]

Così, nell'annosa vicenda 'Amanda Knox' relativa all'omicidio della studentessa americana Meredith Kercher, la Suprema Corte ha scelto di non imboccare la strada della inutilizzabilità della prova, quanto piuttosto quella di un giudizio 'presuntivo' di sostanziale, intrinseca inaffidabilità di qualsivoglia analisi genetica che discenda dal mancato rispetto delle metodiche di repertamento e delle profilassi in materia di inquinamento seguite dalla comunità scientifica di riferimento.[27] In particolare, i giudici di legittimità hanno rilevato che

26 Rif. Valli 2018.

27 Rif. Cass., Sez. V, 27 marzo 2015, n. 36080, in cui la Corte, dopo aver ricordato che affidabile parametro di correttezza dell'attività di ricerca tecnico-scientifica «non può che essere il rispetto degli standards fissati dai protocolli internazionali che compendiano le regole fondamentali di approccio prescritte dalla comunità scientifica, sulla base dell'osservazione statistica ed epidemiologica», ha affermato «più singolare – ed inquietante – è la sorte del gancetto di reggiseno. Notato nel corso del primo sopralluogo dalla polizia scientifica, l'oggetto è stato trascurato e lasciato lì, sul pavimento, per diverso tempo (ben 46 giorni), sino a quando, nel corso di nuovo accesso, è stato finalmente raccolto e repertato. È certo che, nell'arco di tempo intercorrente tra il sopralluogo in cui venne notato e quello in cui fu repertato, vi furono altri accessi degli inquirenti, che rovistarono ovunque, spostando mobili ed arredi, alla ricerca di elementi probatori utili alle indagini. Il gancetto fu forse calpestato o, comunque, spostato (tanto da essere rinvenuto sul pavimento in posto diverso da quello in cui era stato inizialmente notato). Non solo, ma la documentazione fotografica prodotta dalla difesa di Sollecito dimostra che, all'atto della repertazione, il gancetto veniva passato di mano in mano degli operanti, che, peraltro, indossavano guanti di lattice sporchi ...». Sulle problematiche affrontate si veda in dottrina Lupària 2016.

> indipendentemente dal rilievo scientifico, un dato non verificato, proprio perché privo dei necessari connotati della precisione e gravità, non può conseguire, in ambito processuale, neppure la valenza di indizio. Certo, in tale contesto, non è il nulla, da ritenere *tamquam non esset*. Ed infatti, è pur sempre un dato processuale, che, ancorché privo di autonoma valenza dimostrativa, è comunque suscettivo di apprezzamento, quanto meno in chiave di mera conferma, in seno ad un insieme di elementi già dotati di soverchiante portata sintomatica.

Anche in successive pronunce, la Cassazione ha ribadito che l'eccepita inosservanza di regole procedurali prescritte dai protocolli scientifici internazionali in materia di repertazione e prelievo del DNA, di conservazione dei supporti da esaminare nonché di ripetizione delle analisi comporta che gli esiti di 'compatibilità' derivante dalla comparazione dei profili genetici non abbiano carattere di certezza necessario per conferire una valenza indiziante, ma siano suscettibili di apprezzamento solo in chiave di eventuale conferma di altri elementi probatori.[28] Al contempo, la già menzionata inosservanza non comporta l'inutilizzabilità del dato probatorio ove non si dimostri che la violazione abbia condizionato in concreto l'esito dell'esame genetico comparativo fondante il giudizio di responsabilità (rif. Cass., Sez. VI, 24 febbraio 2022, n. 15140, fattispecie in cui la Corte ha ritenuto immune da censure la decisione di merito che aveva attribuito all'imputato l'utilizzo del guanto da cui era stato estratto il DNA, pur se il prelievo non era avvenuto con guanti sterili, stante la mancanza sul supporto di tracce riferibili a soggetti diversi).

Superato il vaglio relativo al rispetto delle norme procedurali e dell'osservanza dei protocolli, l'organo giudicante è chiamato ad un ulteriore momento di valutazione, ossia apprezzare il margine di certezza del giudizio statistico su cui si fondano gli esiti dell'indagine genetica e al cui fine, risulta determinante il calcolo delle probabilità dell'identificazione. La domanda a cui è necessario fornire una risposta scientifica è quella di quanti sono gli individui nella popolazione

28 Cfr. Cass., Sez. II, 6 luglio 2022, n. 38184.

rilevante per il caso di specie che possiedono lo stesso profilo genetico. Ancora una volta, come nello svolgimento delle indagini preliminari, anche nel corso del giudizio, risulterà di fondamentale importanza l'apporto sul punto degli esperti in materia che hanno svolto i relativi accertamenti, il cui sapere scientifico risulterà di grande rilievo ai fini del decidere.

Bibliografia

Biondo 2016: Biondo R., *La Banca dati nazionale DNA italiana*, in Rivista italiana di medicina legale, 2016, 1, 213-232.

Buscemi, Barni 2021: Buscemi L., Barni F., *Genetica forense ed intervento sulla vittima di violenza*, in Rivista italiana di medicina legale, 2021, 4, 1063-1098.

Felicioni 2018: Felicioni P., *Processo penale e prova scientifica: verso un modello integrato di conoscenza giudiziale*, in Cassazione penale, 2018, 4,1620-1648.

Gigli 2019: Gigli F., *Ammissione e valutazione della prova. Il contradditorio risolve in contrasto tra gli esperti e rende superflua la perizia*, in Giurisprudenza italiana, 2019, 11, 2537 ss.

Locard 1920: Locard E., *L'enquête criminelle et les méthodes scientifiques*, Paris 1920.

Lupària 2016: Lupària L., *Le promesse della genetica forense e il disincanto del processualista. Appunti sulla prova del Dna nel sistema italiano*, in Rivista italiana di medicina legale, 2016, 1, 167-177.

Parodi 2022: Parodi C., *La disciplina giuridica delle varie forme di investigazione scientifica. Profilo normativi, giurisprudenziali e prassi applicative*, in Quaderni della Scuola Superiore della Magistratura, 29, 2022, 71-92.

Presciuttini 2019: Presciuttini S., *La prova del Dna fra probabilità e certezza*, Milano 2019.

Previderè, Fattorini 2016: Previderè C., Fattorini P., *La complessità in genetica-forense: l'analisi di DNA in limitata quantità (low copy number DNA) e l'interpretazione di tracce*

commiste, in Rivista italiana di medicina legale, 2016, 1, 179-193.

Rivello 2016: Rivello P., *Alcune osservazioni in ordine alla Banca dati nazionale del Dna*, in Diritto penale e processo, 2016, 11, 1521-1531.

Taroni *et al*. 2018: Taroni F., Bozza S., Garbolino P., *Contaminazioni di un reperto con il DNA. Quando la prova genetica porta direttamente alla condanna?*, in Diritto penale contemporaneo, 2018, 2, 1-15.

Tonini 2003: Tonini P., *Prova scientifica e contraddittorio*, in Diritto penale e processo, 2003, 12, 1459-1465.

Valli 2018: Valli R., *Valutazione dell'affidabilità dell'indagine genetica svolta con violazione di "protocolli" e linee guida: utilizzabilità del risultato raggiunto*, in Diritto penale contemporaneo, 2018, 12, 15-30.

PARTE II

DALLE IMPRONTE DIGITALI AL RICONOSCIMENTO FACCIALE

LE IMPRONTE DIGITALI QUALE METODO IDENTIFICATIVO DALLE ORIGINI AD OGGI

Massimo Taormina
Gabinetto Regionale di Polizia Scientifica di Palermo - Unità di Dattiloscopia Giudiziaria

Abstract: Fingerprints analysis (dactyloscopy) is the study, examination and comparison of fingerprints and / or palmprints left by the dermal drawings with the purpose of identifying a person. The method is applied both in the context of judicial police investigations and in the case of identification of unidentified bodies.

Parole chiave: impronte digitali; dattiloscopia; identificazione.

1. Premessa

La dattiloscopia è lo studio, la catalogazione, l'esame ed il confronto delle impronte lasciate dai disegni dermici (dermatoglifi) presenti sui polpastrelli, sui palmi delle mani e sulla pianta dei piedi con il principale scopo di identificare una persona.

Nel suo significato etimologico più generale il termine 'identità' sottintende un giudizio espresso all'esito di un confronto tra due o più termini che si considerano uguali. Pertanto, l'interpretazione accettabile della locuzione è solo in via 'relativa' ovvero quando l'uguaglianza è riferita ad un soggetto (ma anche ad un oggetto) in ragione dell'analisi di almeno due termini omogenei che lo rappresentano.

Il principio di 'identità assoluta' infatti, sul piano ontologico, non ammette dimostrazione, è una verità elementare riassunta nella definizione "essere sé stesso ed essere; esso è quindi solamente sé stesso". Il duplice concetto – identità assoluta / identità relativa – si può riassumere con l'equazione 0=0.[1] In termini di identità assoluta l'equazione esprime l'individualità (0 uguale a sé stesso 0), ma non esclude che i due elementi dell'equazione (primo e secondo termine), ferma restando la loro individualità in senso assoluto, possano

1 Equazione di Locard.

essere considerati uguali in ragione di ciò esprimono (identità relativa).

2. Un po' di storia

Le proprietà di 'autenticazione' delle impronte papillari sono note empiricamente all'uomo da secoli; si riportano infatti ritrovamenti di documenti di natura commerciale risalenti al VII-VIII secolo d.C., ove nel Sud-est asiatico, a fianco del nominativo del firmatario (in genere analfabeta) veniva apposta una impronta digitale del soggetto, quale 'sigillo autenticativo' della persona che aveva 'firmato' l'atto.

Tuttavia, per giungere ad uno studio analitico, basato su osservazioni oggettive e ripetibili si deve aspettare il XIX secolo.

Spinti dalla corrente di pensiero positivista, numerosi studiosi di diverse nazionalità tentano un approccio 'scientifico' per lo studio e la catalogazione delle impronte digitali, con il principale scopo di poter identificare gli individui, anche a distanza di tempo ed a prescindere dagli eventuali tentativi di dissimulare la propria identità o sostituirsi ad altra persona. Impossibile menzionarli tutti in questa pubblicazione, tuttavia non si possono non ricordare i principali studiosi, che a cavallo tra la seconda metà dell'Ottocento ed i primi del Novecento pongono le basi di tale studio.

Tra i primi a tentare un approccio rigoroso all'analisi delle impronte digitali non può non menzionarsi William James Herschel,[2] che in una lettera del 1877 diretta all'Ispettore generali delle carceri del Bengala ebbe a scrivere:

> … ne ho raccolte a migliaia nel corso degli ultimi 20 anni e sono pronto a rispondere dell'identità di ogni individuo di cui possa produrre le impronte digitali. Vi mando questo saggio poiché sono convinto che l'identificazione nelle prigioni non sia affatto così inutile come si potrebbe essere portati a pensare. L'obiettivo è quello di vanificare ogni tentativo di rinnegare la propria identità o di sostituirsi ad altra persona.

2 William James Herschel (1833-1918), magistrato dell'Impero britannico.

Tra gli studiosi della materia si deve anche ricordare Francis Galton[3] a cui va il merito di raccogliere e rielaborare in un unico saggio,[4] tutti gli studi fatti da altri autori sulla materia, enunciando i principi fondamentali alla base dello studio della moderna dattiloscopia: 'immutabilità', 'unicità e variabilità', 'classificabilità delle impronte digitali'.

Immutabilità: Galton, basandosi anche sugli studi del medico italiano Marcello Malpighi,[5] di oltre due secoli prima, afferma che il derma delle zone cutanee ove sono presenti le creste papillari, ha la proprietà, in caso di lesioni, di rigenerare il disegno in modo perfettamente identico a quello che era presente prima della lesione stessa; pertanto, il disegno delle impronte è immutabile nel tempo, dalla nascita fino ai fenomeni degenerativi *post mortem*.

Unicità e variabilità: basandosi sulle raccolte di impronte fatte da diversi interpreti dell'epoca Galton conclude che, non esistono due impronte digitali uguali (anche nello stesso individuo) ed a corollario di tale osservazione, esse sono quindi "infinitamente variabili".[6]

Classificabilità delle impronte digitali: pur nella loro infinità variabilità, le impronte digitali, per le loro caratteristiche generali, possono essere tutte ricomprese in quattro tipi fondamentali di figure che definisce 'adelta' (o impronte ad arco), 'monodelta' (o impronte aperte), 'bidelta' (o impronte chiuse) e 'bidelta composte' (o impronte a doppio centro di figura).

Tale ultimo principio apre la strada alla creazione di schedari dattiloscopici organizzati, ove è possibile fare una catalogazione e quindi una successiva ricerca delle impronte a fini identificativi, indipendentemente dai dati anagrafici forniti dal soggetto fotosegnalato.

Autorevole studioso della materia è il criminologo francese Edmond Locard.[7] Come altri studiosi del tempo esso intro-

3 *Sir* Francis Galton (1822-1911), antropologo, naturalista, cugino di Charles Darwin.

4 Galton 1892.

5 Malpighi 1665.

6 Tale principio verrà confermato nel tempo dall'ampliarsi dei dati raccolti ed in ultimo dall'utilizzo di sistemi di analisi automatizzati.

7 Edmon Locard (1877-1966): Criminologo, medico legale, fondatore nel 1910 del Laboratorio di Medicina Legale e Polizia Scientifica presso il Palazzo di Giustizia di Lione.

duce, accanto alla misurazione antropometrica, l'acquisizione e lo studio delle impronte digitali come metodica identificativa. Uomo dalla non comune intelligenza, approfondisce gli studi di Polizia Scientifica nei settori della dattiloscopia, della grafica e del sopralluogo. A lui va il merito di aver enunciato per la prima volta il principio dell'interscambio: "Ogni criminale lascia sul luogo del delitto una traccia e porta via con sé una traccia". Tale principio, apparentemente banale, apre a molteplici considerazioni. Il principio dell'interscambio, infatti, non si applica soltanto all'*offender,* ma a qualsiasi attore che interagisce con la scena del crimine. Da qui la necessità di congelare e preservare quanto più possibile il luogo del reato da inquinamenti e consentire l'accesso ai luoghi, ove attuabile, soltanto al personale a conoscenza delle procedure per limitare quanto più possibile l'interscambio e non compromettere le eventuali fonti di prova presenti. Altra considerazione può farsi proprio sulle tracce dell'interscambio, che spesso sono invisibili o molto piccole; ne consegue che è necessario dotare il personale di Polizia Scientifica di una adeguata *process map* di intervento e delle attrezzature idonee che ne consentano la rilevazione e ne evitino la dispersione.

La scena italiana vede come attore protagonista il Prof. Salvatore Ottolenghi.[8]

Influenzato dal sistema di lavoro del suo 'maestro' Cesare Lombroso e dai suoi studi scientifici, Ottolenghi volge la sua attenzione sullo studio del fenomeno criminale e comprende come la 'scienza' possa aiutare le autorità di Polizia nell'analisi del crimine e nella identificazione del reo. Segue con attenzione gli studi dell'epoca su tali materie e le approfondisce già prima della creazione della Scuola di Polizia Scientifica, organizzando nel 1895, da titolare della Cattedra di Medicina legale presso l'Università di Siena, un corso libero di polizia giudiziaria scientifica che si proponeva di fornire ai futuri medici legali e avvocati le nozioni necessarie allo svolgimento delle loro attività.

Esso, pertanto, è in possesso di un notevole bagaglio di studio ed esperienza quando, nel 1902, coglie l'occasione che aspettava. Si presenta dall'allora Capo della Polizia France-

8 Salvatore Ottolenghi (1861-1934), medico legale, allievo e poi collaboratore di Cesare Lombroso, fondatore della Scuola di Polizia Scientifica.

sco Leonardi, proponendo l'idea di fondare una vera e propria scuola di Polizia Scientifica, da far frequentare a tutti i funzionari, ove impartire le nozioni per la raccolta di informazioni utili per l'identificazione dei criminali, sia diretta, che sulla base della raccolta di tracce sui luoghi ove i crimini sono stati commessi. Leonardi accoglie con entusiasmo le idee di Ottolenghi e le rappresenta al Ministro dell'Interno Giovanni Giolitti. È un successo!

Alla fine del 1902, viene organizzato un corso pilota, riservato ad un gruppo ristretto di funzionari di Polizia della Questura di Roma e nell'anno successivo, il 1903, con l'organizzazione del 1° Corso di Polizia Scientifica, nasce ufficialmente la Scuola di Polizia Scientifica.

Da subito Ottolenghi pone tutta la sua attenzione allo studio delle impronte digitali come metodo 'elettivo' per l'identificazione dei rei e delle persone pericolose o sospette, affidando ad un brillante frequentatore del corso del 1902, il Comm. Giovanni Gasti,[9] il compito di ideare un sistema italiano per la classificazione delle impronte digitali. Ottolenghi ebbe a dire: "... non dubitiamo un minuto a pensare ad una classificazione dattiloscopica. Semplice e pratica allo stesso tempo".

Gasti si mise subito a lavoro ideando una classificazione delle impronte digitali che, accanto alla facilità d'impiego, coniugasse un livello di dettaglio tale da poter suddividere i cartellini fotosegnaletici prodotti in due schedari che consentissero una veloce identificazione della persona. Il primo schedario raggruppava le schede segnaletiche in ordine alfabetico, secondo le generalità dei soggetti, mentre il secondo, suddivideva le schede sulla base di un preciso sistema numerico. Il Gasti, basandosi sui quattro tipi fondamentali di figura, ideò una classificazione delle impronte digitali basata su dieci simboli (da 0 a 9) tale da permettere la catalogazione dei cartellini utilizzando una formula numerica[10] con 10 miliardi di possibili combinazioni. Il livello di dettaglio era così spinto da consentire la ricerca di un cartellino e l'identifica-

9 Giovanni Gasti (1869-1939), Commissario di Polizia, poi Questore, frequentatore del Corso di Polizia Scientifica del 1902 e poi collaboratore di Salvatore Ottolenghi all'interno della Scuola di Polizia Scientifica.

10 Formula decadattiloscopica: IPA(sx), IPA(dx), MM(sx), MM(dx), ove IPA sono i simboli attribuiti alle impronte delle dita Indice, Pollice e Anulare e MM sono i simboli attribuiti alle impronte del medio e del mignolo.

zione di una persona, in tempi per l'epoca inimmaginabili. Utilizzata in Italia a partire dal 1904 ed adottata da diverse Polizie nel mondo, fu impiegata fino al 1998 anno di introduzione in Italia del sistema A.F.I.S.[11]

Nasce così l'embrione dell'attuale Casellario Centrale d'Identità, incardinato presso il Ministero dell'Interno-Dipartimento della Pubblica Sicurezza, che raccoglie ancora oggi tutti i fotosegnalamenti effettuati sul territorio nazionale, da tutte le Forze di Polizia abilitate allo scopo.

In una delle sue ultime apparizioni pubbliche, nel corso del 3° Congresso Internazionale di Polizia, tenutosi ad Anversa nel 1930, il Prof. Ottolenghi delineò sinteticamente la sua idea di Polizia Scientifica:

> La Polizia è impegnata in una lotta continua e quotidiana, una lotta impari contro il delitto. In queste condizioni la Polizia empirica, dell'investigatore di strada, ha indubbiamente raggiunto risultati apprezzabili … ma quanto maggiori sarebbero stati quei risultati, se quei funzionari si fossero serviti dei mezzi che dalla scienza avrebbero potuto attingere … tanto più che gli stessi delinquenti sanno invece valersi molto bene dei mezzi che offre il progresso della civiltà. La Scuola di Polizia Scientifica deve avere lo scopo di fornire la cultura tecnica degli argomenti più moderni che riguardano l'accertamento dei reati, l'identificazione e la vigilanza dei rei".

L'attualità delle affermazioni del Prof. Ottolenghi, a distanza di quasi un secolo, non può che sottolineare lo spessore dell'uomo.

3. La dattiloscopia

La dattiloscopia si propone quindi come metodica identificativa solida, rapida, economica, che consente di giungere all'identificazione di una persona, utilizzata oggi anche per scopi estranei all'attività di Polizia Giudiziaria o di Prevenzione.[12]

11 A.F.I.S.: *Automated Fingerprint Identification System*.

12 Si pensi, a titolo di esempio, a dispositivi come smartphone, tablet o PC che 'riconoscono' il proprietario tramite la scansione dell'impronta o ai sistemi

I più recenti studi scientifici consentono di affermare che qualsiasi metodica identificativa di una persona, trae la propria radice dall'unicità del patrimonio genetico di ciascun individuo. Tratti distintivi il colore degli occhi o dei capelli, la forma del viso e tutti gli altri aspetti fisiognomici di un soggetto, hanno la propria origine proprio dall'immenso ed unico patrimonio di dati racchiuso nel D.N.A.

Anche lo sviluppo delle impronte digitali trova la sua fonte in questo patrimonio[13] e parte sin dalla 10-12 settimana di vita intrauterina.

Lo studio dei feti umani ha consentito di osservare che in questa fase della gestazione, sulle zone epidermiche interessate (palmi delle mani e piante dei piedi), iniziano a formarsi microscopiche e flessibili escrescenze dermiche che, con l'avanzare della gravidanza si fondono tra loro formando le creste papillari e con esse il dermatoglifo.

Tuttavia, il patrimonio genetico da solo non spiega integralmente la variabilità delle impronte.

È il caso dei gemelli monozigoti, possessori di identico patrimonio genetico ma di impronte diverse.

Si ritiene che le interazioni dei feti con l'ambiente uterino, soprattutto con il liquido amniotico e con le pareti della placenta nonché di altri fattori (vascolarizzazione del derma, sviluppo del sistema nervoso ecc.) contribuiscano a creare i diversi e casuali posizionamenti delle escrescenze dermiche e successivamente la loro fusione in creste papillari, tanto da giustificare i diversi caratteri delle impronte dei due gemelli, sin dalla nascita. Per cercare una analogia è quello che accade ai granelli di sabbia nel deserto o nel fondo del mare, il cui orientamento risente dell'interazione con fluidi come l'aria o l'acqua.

Ciò che rende possibile lo studio indiretto dei dermatoglifi è dovuto al posizionamento delle ghiandole sudoripare in queste zone di derma. Infatti sui palmi delle mani e sulla pianta dei piedi i pori che secernono l'essudato si posiziona-

di accesso (*biodigit*) che sfruttano tale semplice rilevazione biometrica per consentire l'ingresso dei soggetti autorizzati ad aree private, sensibili o riservate.

13 Si osserva infatti che le patologie che alterano il naturale sviluppo delle creste papillari dipendono da malattie genetiche rare (es. l'adermatoglifia dovuta all'alterazione del gene SMACARD1).

no lungo le creste papillari. Il deposito selettivo di tale liquido sulle creste ne consente poi il rilascio sulle superfici manipolate, in modo da riprodurre il disegno delle stesse.

Lo studio dattiloscopico, nato principalmente per dare una risposta all'esigenza di pervenire ad una identificazione certa dell'individuo (identità preventiva), trova quasi subito applicazione pratica anche in ambito giudiziario. Il cartellino fotodattiloscopico, documento elettivo per l'identificazione preventiva del soggetto, è una preziosa fonte di informazioni anche nella circostanza in cui le impronte contenute il tale documento vengano poste a confronto con i frammenti di impronte papillari documentati sulla scena del crimine su oggetti / superfici manipolate dall'autore del reato. Ancora oggi e nonostante sia noto a tutti il potenziale identificativo delle impronte, una delle fonti di prova materiali che più frequentemente viene documentata sulla scena del crimine sono proprio le impronte papillari.

In tal caso si parla di 'identità giudiziaria' ovvero quando uno dei termini di paragone è sempre l'impronta (anche parzialmente riprodotta) documentata sul *locus commissi delicti*.

Per giungere ad una certa identificazione mediante lo studio delle impronte papillari è necessario approfondire il livello di analisi che non può basarsi esclusivamente sui 'caratteri generali' (o caratteri di 1° livello) dell'impronta, la cui dissomiglianza può comunque fornire un giudizio di NON identità, ma occorre individuare i 'caratteri particolari' (o caratteri di 2° livello), ovvero le accidentalità sulla naturale evoluzione dell'andamento delle creste papillari.

I caratteri particolari o 'minuzie' sono gli elementi che differenziano e rendono uniche le impronte, l'individuazione di un congruo numero di questi caratteri all'interno del disegno dell'impronta, la loro forma e la loro posizione dell'una rispetto alla successiva e l'assenza di dissomiglianze tra gli elementi a confronto, sono i costituenti che si devono valutare per esprimere un giudizio di identica provenienza dei due termini dattiloscopici oggetto di analisi. È proprio il rigoroso tecnicismo da seguire nella fase del confronto, che permette di esprimere il giudizio di identica provenienza.

Per completezza espositiva va inoltre appena introdotta la possibilità di analisi dei 'caratteri microscopici' (o caratteri

di 3° livello). Si tratta principalmente dell'analisi di forma e posizione dei pori delle ghiandole sudoripare presenti lungo le creste papillari. Diversi studiosi (Locard, Faulds e più recentemente Ashbaugh) affermano che, al pari degli altri caratteri, essi hanno le medesime proprietà di immutabilità, unicità e variabilità e quindi sono elementi valutabili ai fini di un giudizio di identità. L'utilizzo di tali caratteri è però nella pratica assai limitato; da un lato per la garanzia identificativa già ampiamente offerta dall'individuazione, più agevole, dei caratteri di 2° livello, dall'altro per la difficoltà di rilevazione e di studio di tali microscopici caratteri. Il loro potenziale utilizzo pratico è pertanto limitato alla rarissima casistica di tracce papillari di esigua superficie (ossia costituite da poche linee) ma così estremamente nitide e nette da consentire l'applicazione di tale studio.

L'analisi delle impronte papillari come metodica identificativa, di pari passo con il ruolo della Polizia Scientifica, si radica e si struttura nel tempo, trovando una costante e sempre maggiore applicazione nella soluzione dei reati. Tuttavia, sin dai primi dai primi anni dello scorso secolo e fino al finire degli anni '90 esso si fonda su una struttura basata essenzialmente su archivi cartacei, ove il dattiloscopico si muove, come un artigiano, con pazienza e rigore metodologico.

Un epocale punto di svolta si ha nella seconda metà degli anni '90 con l'introduzione di software di analisi delle impronte che consentono una ricerca veloce e massiva del dato analizzato tramite comparazione con l'intero archivio di dati, impensabile fino a quel momento con il solo lavoro umano. È la nascita del sistema A.F.I.S. e della informatizzazione del Casellario Centrale d'Identità.

Qualcuno potrebbe essere portato a concludere che la nascita di un imponente archivio informatico porti 'all'estinzione' della figura professionale del dattiloscopista. Tale conclusione è errata.

Per spiegarne i motivi partiamo dall'analisi dell'acronimo A.F.I.S. (*Automated Fingerprints Identification System*) ed in particolare sul significato delle parole 'sistema automatizzato' (e non automatico).

Facendo la doverosa premessa che, chi scrive non è un esperto informatico, il software A.F.I.S. è un prezioso ed inso-

stituibile strumento fornito al dattiloscopista, che consente una ricerca del dato veloce e completo. Tuttavia, il sapere e la metodica tecnica in possesso 'dell'artigiano' permangono, soprattutto nel settore dell'identità giudiziaria ed anzi si affinano ed evolvono. Il sistema, infatti, accanto ad una ricerca totalmente automatica, prevede una fase precedente ed una successiva ove l'intervento dell'operatore è fondamentale ai fini del buon esito delle attività. Nella fase antecedente alla ricerca, infatti, il dattiloscopista analizza la scheda deca-dattiloscopica o il frammento d'impronta da ricercare, indica le caratteristiche generali e particolari, attribuisce ove possibile la classifica, ovvero fornisce i 'corretti' elementi di ricerca al sistema.[14] All'esito della fase di ricerca il sistema fornisce una lista di cartellini o impronte, ovvero quelli maggiormente 'somiglianti' ai caratteri indicati dall'operatore durante la prima fase. Ritorna quindi nuovamente indispensabile il sapere dell'operatore nell'individuare tra i potenziali 'candidati' quello che, all'esito di una rigorosa comparazione, consente di esprimere i giudizi di identità o non identità. Pertanto, per concludere, l'A.F.I.S. è un formidabile strumento d'indagine, ma resta pur sempre uno strumento da porre 'nelle mani' di un operatore specializzato.

L'evoluzione del Casellario Centrale d'Identità, con l'introduzione del sistema A.F.I.S. è quasi copernicana, con tempi di precedentazione ridotti a pochi minuti, impensabili con la ricerca manuale e la comparazione del dato inserito con l'intero archivio in possesso del sistema.

La rilevazione e il confronto delle impronte papillari oltre che per scopi di identificazione preventiva o giudiziaria della persona vivente ha trovato, da subito, un'applicazione pratica anche nei casi di identificazione di cadaveri sconosciuti.

Il tema, morale oltre che giuridico, solo apparentemente anacronistico in una società evoluta come la nostra, è tutt'oggi assai frequente.

Nel marzo del 2008, nella prima relazione semestrale del Commissario straordinario del Governo per le persone scomparse, vengono riportati i dati relativi al cd. censimento dei cadaveri non identificati, richiesto dall'Autorità in questione alla fine del 2007. Veniva verificato il numero dei cadaveri

14 Fase definita del 'controllo qualità'.

ignoti giacenti presso gli obitori comunali e le A.S.L.: "... a Milano e provincia risultano 83 cadaveri, 36 a Roma ...".[15]

Anche in tali occasioni il dato dattiloscopico è quello che più di altri offre certezza, velocità ed economicità del risultato. L'acquisizione delle impronte dal cadavere risulta infatti prassi agevole e non discostante dall'acquisizione da vivente, nei casi in cui tale attività sia svolta a breve distanza temporale dal decesso o su cadaveri adeguatamente conservati. Le metodiche di acquisizione diventano via via più complesse e parziali nei casi di progressione dei diversi tipi di fenomeni degenerativi *post mortem*.

Tuttavia, il principale limite all'identificazione dei cadaveri sconosciuti è dato dalla incompletezza delle banche dati. I *data base* di Polizia, infatti, contengono informazioni (fotografiche, dattiloscopiche, profili genetici, etc.) soltanto di quelle persone che sono state sottoposte a rilievi, nei casi tassativamente previsti dalle norme del C.P.P., del T.U.L.P.S. o del T.U.I. Appare quasi lapalissiano quindi affermare che non sempre, l'acquisizione di elementi identificativi dal cadavere sia poi certezza dell'identificazione dello stesso. L'argomento è assai dibattuto e controverso; una possibile soluzione sarebbe quella di creare una banca dati di impronte digitali estesa a tutti i cittadini / residenti sul territorio nazionale,[16] tuttavia tale ipotesi, tecnicamente valida, rapida ed economica, si scontra con la difficoltà di disciplinare un argomento con diversi e fondamentali interessi contrapposti, da dover bilanciare in un tale tipo di normazione.

4. Gruppi di lavoro permanenti

L'affidabilità del risultato dello studio dattiloscopico, dimostrata ormai da oltre un secolo, trova oggi collocazione in diversi gruppi di lavoro permanenti, nazionali e sovranazionali, sia operativi che di studio / ricerca.

15 Ministero dell'Interno, Relazione semestrale del Commissariato Straordinario per le persone scomparse, marzo 2008, p. 7.

16 Lo stesso Commissario straordinario, nella relazione del marzo 2008, individua la Dattiloscopia tra le prime metodiche identificative dei cadaveri sconosciuti.

Gruppo di missione D.V.I.-Polizia (*Disaster Victim Identification*): istituito con decreto del Capo della Polizia del 6 aprile 2006, ha raccolto l'esperienza maturata dagli operatori della Polizia Scientifica e del servizio sanitario della Polizia di Stato, per l'identificazione dei connazionali presenti nei Paesi investiti dallo Tsunami del 2004. Formato da diverse squadre dislocate su tutto il territorio Nazionale, ogni squadra è composto dalle diverse professionalità necessarie per tali missioni (biologi, dattiloscopisti, operatori esperti del sopralluogo, medici legali). Il gruppo dalla sua nascita è stato attivato in diverse occasioni, per eventi calamitosi e / o disastri su larga scala. L'ultimo intervento del gruppo di missione risale al febbraio 2023, in occasione del terremoto in Turchia.

U.D.I. (Unità Delitti Insoluti)*:* Istituita presso la Direzione Centrale Anticrimine del Dipartimento della Pubblica Sicurezza, con decreto del Capo della polizia del 3 agosto 2009, è composta da personale investigativo dello S.C.O. (Servizio Centrale Operativo) e del Servizio Polizia Scientifica. L'unità è deputata all'analisi, al coordinamento ed alla propulsione delle indagini avviate su casi criminali accaduti in passato e non ancora risolti, anche alla luce delle più recenti metodiche investigative di tipo scientifico.

Gruppo E.N.F.S.I. – EFP-WG (*European Fingerprint – Working Group*): fondato nel 1995, l'E.N.F.S.I. (*European Network of Forensic Science Institute*) è un istituto europeo nato con lo scopo di migliorare lo scambio di informazioni nel campo delle scienze forensi. Oltre che al lavoro generale nei settori della qualità, della gestione delle competenze, della ricerca e dello sviluppo, le diverse professionalità forensi sono trattate da 17 diversi gruppi di lavoro, tra i quali il *Fingerprint Working Group*, con lo scopo di sviluppare e analizzare le competenze nello studio della dattiloscopia presenti nei Paesi aderenti. L'E.N.F.S.I. è stato riconosciuto dalla Commissione europea come 'ente monopolistico' nel campo delle scienze forensi. Il gruppo si riunisce almeno una volta all'anno presso la sede di uno degli organismi europei aderenti, tra i quali il Servizio Polizia Scientifica. Il settore di identità giudiziaria del Servizio Polizia Scientifica è altresì iscritto regolarmente all'esecuzione degli esercizi collaborativi predisposti dal sottogruppo di lavoro '*identification*'.

5. Cooperazione internazionale

Sulla base di diversi accordi, bilaterali o multilaterali, i dati dattiloscopici (sia cartellini fotosegnaletici che i dati raccolti sulle scene del crimine) possono poi essere scambiati tra Paesi aderenti, con lo scopo di contrastare gravi crimini e gestire il fenomeno dell'immigrazione. Si riportano di seguito i principali.

Sistema Informativo Schengen (S.I.S.)*:* firmato il 19 giugno 1990 ed entrato in vigore nel 1995, l'accordo di Schengen aveva come scopo principale quello di abolire i controlli sulle persone e sulle cose alle frontiere degli Stati membri dell'allora Comunità europea, sostituendole con le verifiche effettuate dai singoli Stati alla 'frontiera esterna'. Al vantaggio indubbio di rendere facile la circolazione delle persone e delle cose, si rendeva tuttavia necessario trovare un sistema che rendesse maggiormente effettiva e celere l'individuazione dei criminali e dei proventi dei crimini, in caso di spostamenti di questi da uno stato membro all'altro. Attraverso il S.I.S. i Paesi membri condividono segnalazioni ed una molteplicità di dati in modo da consentire agli Stati di avere informazioni quanto più complete e affidabili. Tra i dati interscambiati, al fine di verificare e confermare l'identità delle persone 'segnalate' nel sistema, vengono resi disponibili elementi quali la fotografia e le impronte digitali e palmari.

Interpol: Organizzazione Internazionale della Polizia criminale, consente l'interscambio di informazioni (anche dattiloscopiche) tra i Paesi aderenti, volte al contrasto del crimine internazionale. Tra i casi di interscambio di dati dattiloscopici mediati dai collaterali Uffici Interpol, si annovera quello della soluzione di una sensazionale rapina, avvenuta nel 2007 presso la gioielleria *Excelsco Diamond* di Tokyo. La valutazione dei frammenti trasmessi dall'Ufficio Interpol giapponese ha consentito infatti l'identificazione di un criminale bosniaco, fotosegnalato in Italia, risultato appartenere al gruppo criminale *Pink Panter*, accusato di aver messo a segno numerose e consistenti rapine in gioiellerie in giro per il mondo, per un danno complessivo quantificato in diversi milioni di euro.

Sistema Eurodac (*European Dactyloscopie*): istituto con il Regolamento (CE) del Consiglio n. 2725/2000 è il database europeo delle impronte digitali per tutti coloro

che richiedono asilo politico, per le persone che varcano irregolarmente una frontiera esterna dell'U.E. e per coloro che soggiornano irregolarmente all'interno di uno dei Paesi dell'U.E. Attraverso tale banca dati e mediante il confronto dattiloscopico è possibile verificare se un cittadino straniero che si trova illegalmente sul territorio di un Paese membro, ha già presentato richiesta di asilo politico in un altro Paese dell'U.E.

6. Considerazioni finali

Con lo studio, l'analisi, la catalogazione ed il confronto delle impronte papillari, nasceva 120 anni fa la Polizia Scientifica. Oggi come allora la dattiloscopia si propone come solida ed affidabile metodica utilizzata per l'identificazione delle persone e per l'individuazione degli autori dei reati.

La tradizione ed i secolari principi di tale studio sono oggi affiancati dai più moderni sistemi forniti dalla tecnologia ed il lavoro quotidiano svolto da operatori dotati di quella 'cultura tecnica' professata e voluta dal suo fondatore, il Prof. Salvatore Ottolenghi.

"Non si umilia la scienza ad occuparsi di Polizia, anzi la si eleva"[17]

Bibliografia

Galton 1892: Galton F., *Finger Prints*, London 1892.

Malpighi 1665: Malpighi M., *De externo tactus organo*, Napoli 1665.

17 Celebre citazione del Prof. Salvatore Ottolenghi.

RICONOSCIMENTO AUTOMATICO DEL VOLTO E CONFRONTO IN AMBITO FORENSE

Giovanni Tessitore
Servizio Polizia Scientifica Roma - Sezioni Indagini Elettroniche

Abstract: Automatic face recognition systems are widely used in our daily lives. The S.A.R.I. project – Automatic Image Recognition System – lauched by the Scientific Police Service of the State Police in 2016, allows for the comparison of facial images with the database of individuals lawfully photographed. However, the results of these searches are not evidential and are always manually verified by qualified operators. Any matches found can be used as support in investigations but do not automatically imply legal meanings.

Parole chiave: riconoscimento facciale automatico; comparazione di immagini facciali; match.

1. Introduzione

I sistemi automatici di riconoscimento del volto hanno assunto un ruolo fondamentale nella nostra quotidianità. Si pensi al loro utilizzo nello sbloccare gli smartphone, nel controllo automatico dei passaporti negli aeroporti, nell'accesso sicuro ai conti bancari tramite sistemi biometrici, o nella gestione dei controlli d'accesso a zone riservate. Le tecnologie in questione non soltanto sono in grado di semplificare le nostre azioni quotidiane, ma contribuiscono anche a garantire una maggiore sicurezza e protezione nelle transazioni e negli ambienti sensibili.

La diffusione generalizzata dei sistemi di riconoscimento facciale in contesti così eterogenei è stata favorita dal costante miglioramento dell'accuratezza del confronto, reso possibile attraverso l'impiego di avanzati algoritmi di intelligenza artificiale. In particolare, un ruolo cruciale ha avuto lo sviluppo delle reti neurali artificiali cd. profonde;[1] ed infatti, a partire dal 2012, con la pubblicazione dei risultati ottenuti con uno dei primi modelli di rete neurale profonda chiamata AlexNet,[2] si è assistito al susseguirsi di modelli analoghi con prestazio-

1 Anche conosciute come '*deep neural networks*'.

2 Krizhevsky *et al*. 2012.

ni via via crescenti che hanno contribuito significativamente al progresso dei sistemi di riconoscimento facciale.[3]

Rispetto alle attività condotte dalle forze di polizia, la costante diffusione dei sistemi di video-sorveglianza, installati soprattutto nelle aree urbane, ha reso sempre più frequente il potenziale impiego dei sistemi di riconoscimento per attribuire una identità al volto ignoto di un soggetto ripreso da una telecamera nell'atto di perpetrare un reato. Tuttavia, l'impiego di tali sistemi da parte delle forze dell'ordine suscita spesso dibattiti riguardo alle questioni legate alla privacy e all'etica ed alla necessità di un bilanciamento accurato tra l'efficacia investigativa degli strumenti introdotti e la tutela dei diritti individuali.

Molto spesso il dibattito è alimentato da preoccupazioni originate da una non completa conoscenza circa l'utilizzo dei sistemi di riconoscimento facciale da parte delle forze di polizia. In questo articolo proveremo a colmare questo 'gap' delineando alcuni ambiti di applicazione di tale tecnologia evidenziandone benefici e limiti di utilizzo.

2. Gli scenari di impiego dei sistemi automatici di riconoscimento facciale

Prima di addentrarci nel merito della tematica è opportuno introdurre i principali scenari applicativi nei quali i sistemi automatici di riconoscimento facciale sono impiegati da parte delle forze dell'ordine.

Ricerca *off-line* o confronto uno-a-molti: in questo scenario una foto di un soggetto con identità ignota viene ricercata all'interno di una banca dati precostituita contenente foto di soggetti con identità nota. L'obiettivo è di trovare una corrispondenza tra la foto del soggetto con identità ignota e una delle foto contenute nella banca dati in modo da pervenire all'identificazione del soggetto ignoto. Questo scenario si concretizza, ad esempio, quando a seguito della commissione di un reato, le forze dell'ordine recuperano immagini dell'autore da un sistema di video-sorveglianza che ha ripre-

3 Parkhi *et al*. 2015.

so l'evento criminoso che vengono poi ricercate all'interno di una banca dati. Nel nostro paese, come vedremo nel seguito, è possibile impiegare sistemi automatici di riconoscimento del volto per la ricerca, uno-a-molti, all'interno della banca dati AFIS[4] dei soggetti foto-segnalati a norma di legge.

Confronto forense o confronto uno-a-uno: in questo scenario l'obiettivo è di stabilire se la foto di un 'soggetto di interesse' con identità ignota corrisponde alla foto del volto di un soggetto con identità nota o di un sospettato. Tale scenario si concretizza, ad esempio, quando a seguito della commissione di un reato, le forze dell'ordine recuperano immagini dell'autore e successivamente, durante lo sviluppo delle indagini, individuano anche un possibile sospettato, di cui sono disponibili una o più foto del volto. In questo scenario, si vuole stabilire se, in termini forensi, il soggetto ripreso nelle immagini – soggetto di interesse – ed il sospettato siano effettivamente la stessa persona, attraverso un confronto uno-a-uno. In considerazione dell'uso dibattimentale di tale confronto, è cruciale che il risultato di questa verifica sia adatto per l'utilizzo in un contesto forense. Vale la pena anticipare che in tale scenario ad oggi non è possibile fare ricorso a sistemi di riconoscimento automatico come sarà spiegato nel seguito dell'articolo.

Ricerca *real-time*: in questo scenario la cd. *watchlist* – una lista di foto di soggetti da vagliare – è confrontata in tempo reale con tutti i volti individuati in uno o più flussi video provenienti da altrettante telecamere. Se un volto, individuato nel flusso video, è sufficientemente simile ad uno presente nella *watchlist*, secondo un indice di somiglianza configurabile, viene generato un '*alert*'. Vedremo che sistemi di questo tipo sono quelli che suscitano le maggiori preoccupazioni riguardo alle questioni legate alla privacy e alla tutela dei diritti individuali e per i quali sono previste delle limitazioni nella bozza di Regolamento UE sull'Intelligenza Artificiale. Infatti, tali sistemi rientrano nell'alveo di quelli per il *Remote Biometric Identification* (RBI) da distinguere da un'altra categoria di sistemi conosciuta come '*post remote biometric identification systems*'. Nei primi, la cattura del flusso video, i confronti e gli eventuali

4 AFIS è l'acronimo di *Automatic Finger Identification System*. Si tratta della stessa banca dati delle impronte digitali. Infatti, all'atto del fotosegnalamento vengono non solo memorizzate le impronte digitali del soggetto ma anche una foto frontale e del profilo-destro.

alert avvengono tutti in tempo reale o con ritardo trascurabile; nei sistemi '*post*', invece, i confronti e l'identificazione avvengono con notevole ritardo rispetto alla cattura dei flussi video.

Nelle figure 1 e 2, sono riportati degli schemi riassuntivi degli scenari applicativi appena descritti.

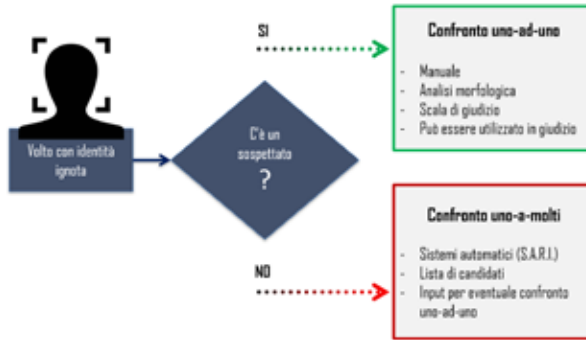

Figura 1: Il confronto uno-a-molti è impiegato quando non si ha a disposizione il volto di un sospettato. In questo scenario sistemi automatici come il S.A.R.I. (che vedremo nel seguito) sono usati per cercare un possibile candidato. Nel confronto forense (o confronto uno-ad-uno), invece, l'obiettivo è di stabile se il volto ignoto ed il volto del sospettato appartengono allo stesso soggetto.

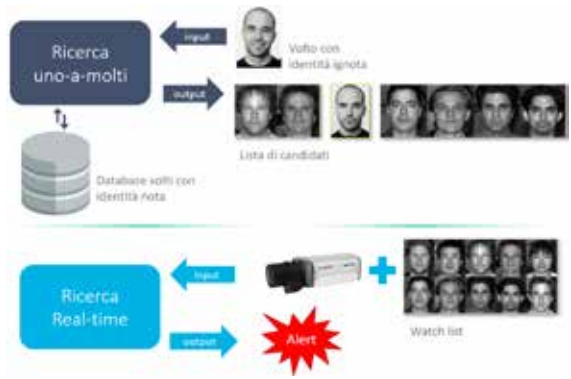

Figura 2: Nella ricerca *off-line* (confronto uno-a-molti) la singola foto di un soggetto di interesse viene ricercata all'interno di una banca dati di voti con identità nota. Nella ricerca *real-time*, invece, tutti i volti presenti in uno o più flussi video vengono confrontati in tempo reale e in maniera continua con i volti presenti in una *Watch-list*. Nel caso in cui uno dei volti del video raggiunga un punteggio di somiglianza rispetto a quelli presenti nella *Watch-list* superiore ad una certa soglia il sistema genera un *alert*.

3. Il sistema S.A.R.I.

A partire dal 2016,[5] il Servizio Polizia Scientifica della Direzione Centrale Anticrimine della Polizia di Stato ha sviluppato il progetto S.A.R.I. – Sistema Automatico Riconoscimento Immagini. Il progetto ha previsto la creazione di due componenti distinte e separate: S.A.R.I. *Enterprise* e S.A.R.I. *Real-Time* di cui accenneremo di seguito.

Il sistema S.A.R.I. *Enterprise* permette di effettuare un confronto uno-a-molti attraverso la ricerca della foto del volto di un soggetto ignoto all'interno della banca dati AFIS della Polizia di Stato, costituita, ad oggi, da circa 20 milioni di foto – presenti sui cartellini fotosegnaletici – e circa 10 milioni di soggetti acquisite in adesione alla normativa vigente.

La soluzione S.A.R.I. *Enterprise* è stata avviata in esercizio nel settembre del 2018 a seguito del provvedimento favorevole del Garante per la protezione dei dati personali n. 440 del 26.07.2018.[6]

È opportuno ribadire che tale sistema non è connesso ad alcun altro sistema né tantomeno a telecamere di video-sorveglianza. Le immagini da ricercare devono essere preventivamente individuate ed estrapolate dalle forze di polizia per poter essere successivamente ricercate.

Il S.A.R.I. utilizza due algoritmi di riconoscimento facciale, di cui uno presente nella lista degli algoritmi testati dal N.I.S.T.[7] denominato *NeuroTechnology*, aggiornati alle ultime versioni disponibili sul mercato e permette di effettuare due tipologie di ricerca con la foto del volto: ricerca per sola immagine: in questa modalità l'utente inserisce, per la ricerca, esclusivamente la foto del volto del soggetto ignoto;

ricerca combinata: in questa modalità l'utente inserisce, per la ricerca, sia l'immagine del volto del soggetto ignoto sia filtri testuali relativi, ad esempio, ai dati anagrafici, alle caratteristiche fisiche, al luogo del fotosegnalamento. Si specifica che questi dati sono acquisiti a norma di legge in fase di fotosegnalamento.

5 https://www.poliziadistato.it/articolo/15557c52775a3724103220539.

6 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9040256.

7 *National Institute of Standard Technology*.

Così come avviene nel caso di altri sistemi che sfruttano parametri biometrici (come le impronte digitali), il risultato di una ricerca uno-a-molti, effettuata mediante un sistema automatico, è una lista di candidati ovvero una serie di volti – in genere 50 – ordinati secondo un valore di similarità, denominato *score*, rispetto al volto del soggetto di interesse.

È opportuno precisare che lo *score* non ha alcuna validità ai fini dibattimentali e la lista dei candidati è sempre verificata da un operatore con specifica formazione per individuare l'eventuale presenza di un soggetto con caratteristiche facciali assimilabili a quelle del volto ignoto. Questa eventuale corrispondenza non ha alcuna conseguenza automatica ma viene utilizzata dagli uffici operanti per il prosieguo dell'attività investigativa.

La revisione manuale dei risultati da parte di un operatore permette anche di mitigare gli effetti prodotti da eventuali *bias* presenti negli algoritmi di riconoscimento facciale in adesione ai principi dell'etica dell'IA, sistemi non discriminanti ed equi.[8]

Nel caso in cui venga individuata dall'operatore una potenziale corrispondenza, affinché essa possa assumere valore probatorio, è necessario procedere ad un ulteriore accertamento tecnico di comparazione fisionomica descritto nel paragrafo successivo.

Le potenzialità di sistemi come il S.A.R.I. si sono manifestate in modo evidente nell'individuazione del responsabile di un accoltellamento ai danni di una ragazza israeliana avvenuto nel 2022 all'interno della Stazione Termini di Roma. L'evento fu ripreso dalle telecamere del sistema di videosorveglianza della stazione, le quali hanno inquadrato anche il volto dell'aggressore. Il sistema di riconoscimento facciale S.A.R.I. ha permesso di effettuare una ricerca all'interno della banca dati dei soggetti fotosegnalati, restituendo una lista di possibili candidati. Questa lista, analizzata dall'operatore di polizia, ha permesso di individuare, tra i cinquanta candidati restituiti dal sistema, l'identità del presunto responsabile. È importante sottolineare il contributo fondamentale sia dell'intelligenza artificiale per la ricerca, sia dell'operatore

8 https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

che è riuscito a individuare una potenziale corrispondenza tra i candidati.

Questa corrispondenza è stata poi oggetto di un ulteriore accertamento di confronto fisionomico.

4. Il confronto uno-a-uno o cd. confronto fisionomico

Nell'ambito forense, in particolare nel confronto del volto uno-a-uno, noto anche come confronto fisionomico, nonostante la diffusione dei sistemi di riconoscimento automatico sopra descritti, è impiegata una metodologia manuale effettuata da un operatore esperto, in accordo a procedure consolidate a livello internazionale e basate sulla tecnica della cd. analisi morfologica.

Il risultato di tale processo, che stabilisce il livello di corrispondenza tra il volto di un soggetto di interesse con identità ignota, rispetto al volto di un sospettato con identità in genere nota, è un giudizio soggettivo di verosimiglianza tra i volti esaminati, espresso su una scala di valori.[9]

Prima di descrivere nel dettaglio come avviene la comparazione attraverso l'analisi morfologica, è bene evidenziare come in effetti, nonostante si tratti di un confronto manuale, il processo di comparazione, differentemente da quanto ci si potrebbe aspettare, è un'attività molto complessa.

Infatti, sebbene l'esperienza quotidiana ci suggerisca che riconoscere volti è un'azione che tutti siamo in grado di effettuare velocemente e senza fatica, va specificato che in realtà esiste una profonda differenza se quest'attività di riconoscimento è rivolta a volti cd. familiari piuttosto che a volti 'non-familiari'. Nel primo caso si tratta di parenti, amici, colleghi, celebrità, ecc. per i quali si è raggiunta, appunto, una familiarità del volto, e che la maggior parte delle persone è in grado di riconoscere con un livello di accuratezza molto elevato anche in immagini di scarsa qualità. Nel secondo caso, invece, si tratta di volti 'nuovi' per i quali, in genere, si è estremamente inaccurati nel riconoscerli e confrontarli.[10] In particolare, la letteratu-

9 ENFSI, 2018.

10 Bruce *et al*. 1999.

ra scientifica dimostra che, "con una comparazione olistica,[11] sussistono forti differenze nella capacità di confrontare volti familiari piuttosto che volti non familiari".[12]

Esistono, tuttavia, alcuni individui, cd. super-riconoscitori,[13] che hanno delle capacità particolari e riescono a riconoscere in maniera accurata anche volti non familiari.[14] Il confronto fatto da questi soggetti, in maniera olistica, non è adatto ad un uso forense in quanto gli stessi non sono in grado di specificare quali caratteristiche del volto li hanno condotti ad una certa conclusione.

Ritornando al problema del confronto uno-ad-uno che abbia validità in ambito forense, vale la pena intanto specificare che si tratta di confronto fatto su volti non familiari. Come specificato precedentemente e come indicato nelle *Best Practices* sul tema emanate dall'E.N.F.S.I.,[15] la metodologia olistica è assolutamente da evitare in questo contesto come pure altre metodologie quali la sovrapposizione o il confronto antropometrico.

È invece opportuno procedere con la comparazione morfologica. Si tratta di un processo in cui le caratteristiche facciali sono osservate e comparate singolarmente evidenziandone differenze o similitudini. Tipicamente è usata una lista predeterminata (*checklist*) di caratteristiche in modo da strutturare e documentare la comparazione. Ad esempio, la *checklist*[16] sviluppata dal '*Facial Identification Scientific Working Group*' (FISWG) è ampiamente adottata dagli istituti forensi europei ed americani.

Nella citata *checklist*, le parti del volto descritte come 'componenti' sono suddivise in dettagliate caratteristiche dette 'sottocomponenti'. Studi empirici[17] hanno mostrato

11 Confrontare in maniera olistica significa guardare i volti nel loro complesso sfruttando l'innata abilità di riconoscimento del cervello umano.

12 Burton *et al*. 1999; Bruce *et al*. 1999.

13 Russell *et al*. 2009.

14 https://greenwichuniversity.eu.qualtrics.com/jfe/form/SV_0wkAa97GeC3ABUO.

15 *European Network of Forensic Science Institutes*, 2018.

16 FISWG 2012 – *Facial Identification Scientific Working Group* (2012). *Guidelines for facial comparison methods*, in https://www.fiswg.org/document/viewDocument?id-25. Vegter *et al*. 2000; Ottolenghi 1910.

17 Towler *et al*. 2017.

che conducendo una comparazione caratteristica per caratteristica si migliora l'accuratezza della comparazione.

La Polizia Scientifica, a partire dal 2018 ha sviluppato, sulla base delle *Best Practices* ENFSI, le proprie linee guida sul confronto fisionomico uniformando su tutto il territorio nazionale questo tipo di accertamento tecnico.

La linea guida prevede un giudizio finale su una scala di sette valori di cui 3 gradi di giudizio positivi, 3 negativi ed uno inconcludente come nella tabella seguente:

Scala di valutazione del confronto fisionomico		
+3	Sostegno estremamente forte	ipotesi accusatoria (immagini del volto ignoto e del sospettato appartenente allo stesso soggetto)
+2	sostegno forte	
+1	sostegno moderato	
0	nessun sostegno	
-1	sostegno moderato	ipotesi difensiva (immagini del volto ignoto e del sospettato appartenenti a soggetti diversi)
-2	sostegno forte	
-3	sostegno estremamente forte	

5. Il confronto uno-ad-uno con sistemi automatici

Come anticipato nei paragrafi precedenti, nella ricerca uno-a-molti, a ciascun elemento della lista di candidati viene assegnato uno *score* che indica il grado di similarità su una scala percentuale.

A prima vista, potrebbe sembrare ragionevole utilizzare questo valore come supporto per la corrispondenza dei volti in un contesto dibattimentale, tanto più che appare come un dato numerico di facile comprensione. Tuttavia, è importante

sottolineare che tale valore è, invece, difficilmente interpretabile in quanto gli algoritmi di confronto automatico sono assimilabili a delle '*black box*'. Ciò significa che non è possibile determinare, ad esempio, quali specifiche caratteristiche del volto abbiano influenzato maggiormente il risultato finale o, più in generale, spiegare le ragioni di un certo punteggio percentuale.[18] Di fatto, nonostante i sistemi automatici di riconoscimento siano impiegati con successo da anni per la ricerca uno-a-molti in un *database*, nel confronto uno-ad-uno o confronto fisionomico, lo '*score*' non può essere portato a sostegno della 'corrispondenza' o della 'non corrispondenza' tra il volto di un sospettato ed il volto di un soggetto di interesse.

Per coloro che non sono esperti del settore, questa differenza di approcci potrebbe risultare sorprendente. Nel seguito proveremo ad illustrare le ragioni tecniche per cui, allo stato attuale, i sistemi automatici non possono essere impiegati per condurre confronti fisionomici ai fini forensi.

È fondamentale precisare sin dall'inizio che queste ragioni non sono correlate all'accuratezza. Infatti, anche il confronto fisionomico, eseguito manualmente da un operatore esperto, fornisce livelli di precisione che, come già accennato, non sono perfetti.[19]

Per comprendere meglio quanto affermato è necessario addentrarci in maniera più approfondita nella tematica cominciando ad osservare che nel confronto fisionomico possono verificarsi le seguenti due ipotesi:

- ipotesi accusatoria (H_A) = il volto del sospettato e il volto del soggetto di interesse appartengono alla stessa persona;
- ipotesi difensiva (H_D) = il volto del sospettato e il volto del soggetto di interesse appartengono a due persone differenti.

Seguendo i dettami dell'*European Network of Forensic Science Institutes*,[20] il compito dello scienziato forense, in

18 Lo *score* è impiegato principalmente nel contesto biometrico. Ad esempio, nello sblocco di un cellulare, lo *score* misura la similarità tra il volto in quel momento inquadrato dal telefono e il modello biometrico precedentemente salvato nel dispositivo. Se lo score supera una certa soglia allora viene dato accesso al sistema (in questo caso al telefono). La soglia viene scelta a seconda della specifica applicazione biometrica in modo da avere determinate prestazioni di falsi positivi (FPR) e falsi negativi (FNR).

19 Philips *et al*. 2018.

20 ENFSI 2016.

questo contesto, è quello di quantificare, anche in maniera soggettiva, la cd. forza dell'evidenza rispetto alle due ipotesi sopra formulate.

Per poterla stimare è necessario valutare due quantità: la similarità tra il volto del sospettato e quello del soggetto di interesse e la tipicità del volto del sospettato rispetto ad una opportuna popolazione di riferimento.

Per illustrare i concetti di similarità, tipicità e popolazione di riferimento si può far ricorso al seguente esempio.

Consideriamo il confronto dell'altezza di un soggetto di interesse, ripreso da un sistema di videosorveglianza, con l'altezza di un sospettato e supponiamo di avere i seguenti due casi:

- CASO 1: il soggetto di interesse ha un'altezza stimata di 174 cm ± 3 cm mentre il sospettato è alto 176 cm;
- CASO 2: il soggetto di interesse ha un'altezza stimata di 200 cm ± 3 cm mentre il sospettato è alto 202 cm.

Supponiamo, inoltre, che il sospettato sia un uomo di nazionalità italiana (altezza media della popolazione maschile italiana pari a 176 cm).

Ci si domanda in quale dei due casi la stima dell'altezza fornisce un contributo maggiore alle indagini ed eventualmente alle successive fasi dibattimentali per l'individuazione dell'autore del reato?

In effetti, in entrambi i casi (ignorando la differenza di errore relativo), la similarità tra l'altezza del soggetto di interesse e il sospettato è la stessa (2 cm). Tuttavia, anche intuitivamente, consideriamo più significativo il CASO 2, poiché l'altezza del sospettato è atipica (bassa tipicità) rispetto alla media della popolazione maschile italiana. Senza rendersene conto, nel tentativo di rispondere al quesito, abbiamo istintivamente considerato il concetto di popolazione di riferimento e di tipicità, valutando correttamente la forza dell'evidenza come rapporto tra la similarità e la tipicità. Questo schema di ragionamento è, peraltro, alla base di ogni confronto in ambito forense.

Ritornando, quindi, al problema iniziale dell'utilizzo dei sistemi automatici per il confronto fisionomico, lo *score* rappresenta solo una misura della similarità tra i due volti a confronto e pertanto risulta insufficiente per un uso dibattimentale. Infatti, nel parallelo con la stima dell'altezza, utilizzare lo *score* sarebbe come conoscere la sola differenza tra l'altezza

del soggetto di interesse e quella del sospettato (2 cm nell'esempio precedente) senza alcuna informazione aggiuntiva circa la frequenza dell'altezza del sospettato tra la popolazione di riferimento.

Per un utilizzo forense, invece, occorrerebbe anche una stima della tipicità dello *score* per il sospettato ovvero conoscere, mediamente, quale *score* ottiene l'immagine del sospettato rispetto alle immagini di una opportuna popolazione di riferimento.

In conclusione, allo stato dell'arte, il valore di *score* fornito da sistemi automatici di riconoscimento dei volti non è idoneo ad un utilizzo forense ma va affiancato da un confronto fisionomico diretto (uno-a-uno) effettuato da un operatore esperto.[21]

6. I sistemi biometrici remoti *Real-Time*

La componente S.A.R.I. *Real-Time* permette l'analisi in tempo reale dei flussi video provenienti da una o più telecamere al fine di generare un *alert* nel caso in cui uno dei volti presenti nei video analizzati sia sufficientemente simile ad uno dei volti caricati nella cd. *watchlist*. Quest'ultima contiene un elenco di foto di soggetti da prendere in considerazione.

Riguardo al sistema S.A.R.I. *Real-Time* va specificato che si tratta di un'unica soluzione tecnologica completamente separata da altri sistemi, compreso il S.A.R.I. *Enterprise*, da installare temporaneamente ed in una zona spazialmente limitata. L'impiego di tale sistema sarebbe sempre circoscritto ad un periodo limitato nel tempo e ad una area di interesse ristretta e ben delineata, ove sarebbero state installate, in maniera momentanea e disgiunta da qualsiasi altro impian-

21 Merita segnalare che è possibile stimare la forza dell'evidenza a partire dallo *score*. Nello specifico, nell'ambito del Framework Bayesiano, la forza dell'evidenza è formalizzata come rapporto di verosimiglianza (*likelihood ratio*, LR) tra la distribuzione dello *score* (s), data l'ipotesi accusatoria, e la distribuzione dello score, data l'ipotesi difensiva [Ali et al. 2010]. Tuttavia, il calcolo matematico di tali distribuzioni presenta, allo stato dell'arte, notevoli difficoltà tecniche soprattutto in relazione alla scelta di una idonea popolazione di riferimento ed alla necessità che tutto il materiale in esame sia omogeneo in termini di qualità delle immagini (risoluzione, compressione, illuminazione, posa del volto, ecc.).

to di videosorveglianza, un numero massimo di dieci telecamere connesse direttamente all'infrastruttura.

In esito all'esame della 'valutazione di impatto sulla protezione dei dati personali (DPIA)', il Garante, con provvedimento n. 127 del 25.03.2021, ha espresso parere negativo all'utilizzo del sistema e conseguentemente, il sistema SARI *Real-Time* non mai è entrato in funzione.

I sistemi di riconoscimento facciale *Real-Time* rientrano nella categoria dei sistemi di identificazione biometrica remota (RBI). Questi sistemi, quando impiegati in luoghi pubblici e per scopi di '*law enforcement*' sono classificati, dalla bozza di regolamento europeo sull'intelligenza artificiale,[22] come pratica di AI proibita. Tuttavia, sono previste delle eccezioni che ne permettono comunque l'impiego sebbene limitato nel tempo e nel luogo nei casi di: ricerche mirate di vittime (rapimento, traffico, sfruttamento sessuale), prevenzione di una minaccia terroristica specifica e attuale, o localizzazione o identificazione di una persona sospettata di aver commesso uno dei reati specifici menzionati nel regolamento (tra cui terrorismo, traffico di esseri umani, omicidio, stupro).

Va specificato che è prevista una preventiva autorizzazione da parte dell'autorità giudiziaria.

7. Intelligenza artificiale e *Deep Fake*: minacce e opportunità

Negli ultimi anni, l'avanzamento della tecnologia nell'ambito dell'intelligenza artificiale e dell'apprendimento automatico ha dato vita a tecniche sofisticate per la generazione di materiale multimediale sintetico, con particolare enfasi sulla generazione di immagini e nello specifico anche di volti.

Una delle problematiche più preoccupanti emerse da questi progressi è la creazione di contenuti *deep fake*, ovvero di media digitali altamente realistici. Ad esempio, nelle foto seguenti sono riportati sei volti generati artificialmente[23] tra-

22 https://www.europarl.europa.eu/pdfs/news/expert/2023/12/press_release/20231206IPR15699/20231206IPR15699_en.pdf.

23 https://thispersondoesnotexist.com.

mite algoritmi di apprendimento profondo, nello specifico facendo ricorso a reti neurali generative avversarie (GAN).

Figura 3: Esempi di volti artificiali.

Nel contesto del confronto forense del volto e dell'uso dei sistemi automatici di riconoscimento facciale, il fenomeno dei *deep fake* rappresenta una sfida significativa e potenzialmente minacciosa. L'uso dei *deep fake* nel contesto delle attività criminali, infatti, potrebbe consentire ad attori malevoli di fabbricare prove incriminanti o manipolare le tracce digitali, mettendo in dubbio l'autenticità e l'integrità delle prove digitali. Per tale ragione, nel prossimo futuro, sarà sempre più importante disporre di dati che siano certificati all'origine o, nel caso di dati provenienti da fonti aperte, disporre di strumenti efficaci per poterne verificare l'autenticità e la genuinità.

Le tecniche di intelligenza artificiale appena descritte possono costituire, tuttavia, anche una opportunità per le forze di polizia. Recentemente, il Servizio Polizia Scientifica ha sviluppato e reso operativo un applicativo, denominato 'AIM4SIE' (*Artificial Intelligence Methods for Smart Investigation of Evidence*), attraverso il quale sono raggiungibili diversi strumenti di IA espressamente sviluppati per fornire un supporto tecnico alle indagini tra cui:

l'elaborazione di identikit: grazie agli algoritmi di IA è possibile generare volti realistici sulla base degli elementi forniti dai testimoni. Il software poi consente di modificare

rapidamente le diverse caratteristiche del volto in base ai ricordi delle vittime. Va specificato, comunque, che anche con l'impiego di strumenti informatici, l'identikit richiede sempre che un esperto della Polizia Scientifica stabilisca una connessione empatica con la vittima e la guidi nel dare forma ai suoi ricordi, spesso associati a esperienze traumatiche;

l'*age progression*: si tratta della possibilità di 'invecchiare' un volto a partire da foto del passato, al fine di stimare come potrebbe apparire attualmente. Questa metodologia riveste un'importanza significativa nelle indagini mirate a individuare latitanti, quando si dispone solo di fotografie datate, o nell'ambito della ricerca di persone scomparse, in cui i familiari forniscono materiale fotografico a disposizione. Il software sviluppato dalla Polizia Scientifica consente non solo di generare volti realistici al variare del grado di invecchiamento ma anche di tenere conto delle caratteristiche legate all'invecchiamento dei familiari del soggetto.

8. Conclusioni

Le sfide tecnologiche che la Polizia Scientifica si troverà ad affrontare nel prossimo futuro riguarderanno senza dubbio lo sviluppo e la diffusione sempre più ampia dei sistemi di intelligenza artificiale, tra i quali quelli legati al riconoscimento facciale. L'impiego di tali tecnologie, soprattutto in ambiti tanto delicati come quello forense, solleva una serie di interrogativi fondamentali riguardanti la validità e l'affidabilità delle evidenze prodotte, nonché la possibilità di comprendere il processo che porta a determinati risultati. Attualmente, molti dei sistemi utilizzati, in particolare quelli basati su tecniche di *deep learning*, agiscono come delle 'scatole nere', rendendo difficile o addirittura impossibile comprendere il ragionamento che li porta a emettere determinate conclusioni a partire da specifici *input*. Questa opacità solleva legittime preoccupazioni riguardo alla trasparenza e alla giustificazione dei risultati ottenuti.

In risposta a queste sfide, negli ultimi anni si è sviluppata una linea di ricerca dedicata alla creazione di sistemi di intelligenza artificiale spiegabili, noti come *Explainable Artificial*

Intelligence (XAI). Questi sistemi si propongono di rendere trasparente il processo decisionale dell'IA, consentendo agli esperti forensi di comprendere e validare le conclusioni raggiunte e, di conseguenza, di utilizzare in modo più sicuro ed efficace le tecnologie di intelligenza artificiale nel contesto forense.

Bibliografia

Bruce *et al*. 1999: Bruce V., Henderson Z., Greenwood K., Hancock P.J.B., Burton A.M., Miller P., *Verification of face identities from images captured on video*, in J. Exp. Psychol. Appl., 5.4, 1999, 339-360.

Bruce *et al*. 2001: Bruce V., Henderson Z., Newman C., Burton A.M., *Matching identities of familiar and unfamiliar faces caught on CCTV images*, in J. Exp. Psychol. Appl., 7.3, 2001, 207-218.

Burton *et al*. 1999: Burton A.M., Wilson S., Cowan M., Bruce V., *Face recognition in poor-quality video: evidence from security surveillance*, in Psychological Science, 10.3, 1999, 243-248.

Krizhevsky *et al*. 2012: Krizhevsky A., Sutskever I., Hinton G.E., *ImageNet classification with deep convolutional neural networks*, in NIPS, 2012, 1106–1114.

Ottolenghi 1910: Ottolenghi S., *Trattato di polizia scientifica*, Milano 1910.

Parkhi *et al*. 2015: Parkhi O.M., Vedaldi A., Zisserman A., *Deep face recognition*, in bmvc. 1.3, 2015.

Philips *et al*. 2018: Phillips P.J., Yates A.P., Hu Y., Hahn K.A., *Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms*, in Proceedings of the National Academy of Sciences, 115.24, 2018, 6171-6176.

Russel *at al*. 2009: Russell R., Duchaine B., Nakayama K., *Super-recognizers: people with extraordinary face recognition ability*, in Psychonomic bulletin & Review, 16.2, 2009, 252-257.

Towler *et al*. 2017: Towler A., White D., Kemp R.I., *Evaluating the Feature Comparison Strategy for Forensic Face Identification*, in J. Exp. Psychol. Appl., 23.1, 2017, 47-58.

IL RICONOSCIMENTO FACCIALE: NUOVE SFIDE NEL PROCESSO PENALE

Annalisa Mangiaracina
Università degli Studi di Palermo

Abstract: AI and especially facial recognition tecniques 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 facciale[2] 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 maschera[5] – 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 privacy[8] 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 GPDP, 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-segnaletiche 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 privacy[13] 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 GPDP, Parere sul sistema "*SARI-Enterprise*", n. 440, 25 luglio 2018.

13 GPDP, 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 privacy[14] 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 GPDP, 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 complementarietà. 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 Cedu; 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 appello[16] 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 omesso 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 suggerito[19] 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 Regolamento[21] 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, "individua[re]", "localizza[re]" 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 "punibil[i] 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 futuribili 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 authomated data exchange for police cooperation* ('Prum II'), 2 marzo 2022.

24 Quattrocolo: 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.

Quattrocolo 2020: Quattrocolo 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.

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.

IL RICONOSCIMENTO AUTOMATICO DEL VOLTO TRA ESIGENZE INVESTIGATIVE E TUTELA DELLA PRIVACY

Pierangelo Padova
Tribunale di Palermo

Abstract: The paper is aimed at exploring the role of facial recognition instruments during the stage of preliminary investigations, taking into consideration their impact on fundamental rights of person under investigation.

Parole chiave: privacy; Clearview; riconoscimento facciale.

1. Introduzione

Per tentare di inquadrare correttamente il tema in esame, pare necessario porsi alcune domande preliminari: qual è il fondamento scientifico delle tecniche di identificazione biometrica? È possibile prevedere quale sarà l'impatto delle tecnologie di riconoscimento del volto sulle indagini di polizia giudiziaria e sulla privacy dei cittadini?

Ma, prima ancora, sorge spontanea una domanda ancor più generale: cosa è la scienza? Cosa è la tecnologia? Ovviamente, non si può neanche pensare, in questa sede, anche solo ad abbozzare una risposta minimamente esaustiva.

Per introdurre l'argomento, si può però fare riferimento alla definizione – riferita alla tecnologia ma adatta, per certi versi, anche alla scienza – proposta dal notissimo scrittore di fantascienza Isaac Asimov, secondo il quale la tecnologia è, in fondo, l'uso di un qualunque strumento in grado di amplificare una facoltà ovvero una capacità dell'essere umano.

I sistemi di riconoscimento automatico del volto, comunemente denominati 'tecniche di riconoscimento facciale' o, sinteticamente, 't.f.r.', sono in grado di amplificare la capacità innata di ogni essere umano di riconoscere il volto umano e di distinguere un volto da un altro.

L'immagine del volto, d'altra parte, dà origine ad un 'dato biometrico', anzi al dato biometrico 'per eccellenza, come si ricava dalla previsione normativa contenuta nell'art. 4, n. 14, del

Regolamento UE/2016/679;[1] da altro punto di vista, che peraltro è anche quello di questo breve contributo, occorre considerare che le discipline tecnico-scientifiche su cui si basano le tecniche biometriche (così come, del resto, le moltissime altre che non è neanche possibile citare in questa sede) possono assumere importanza decisiva in una indagine penale.

La conseguenza è immediata ed intuitiva: è necessario individuare un punto di equilibrio tra l'uso di una determinata tecnologia e la tutela dei diritti individuali, i quali inevitabilmente vengono coinvolti dall'avvio di un procedimento penale, specie se in tale ambito vengono utilizzati strumenti invasivi.

Un ulteriore profilo da considerare è che la nostra epoca – ormai da molti anni e come forse mai nel passato – sembra caratterizzata dal fronteggiarsi di due 'forze' contrapposte: da un lato il principio della divisione del lavoro, per il quale, a causa della crescente complessità delle attività che ciascuno deve svolgere, si viene spinti verso il maggior grado possibile di specializzazione; dall'altro lato una intensa coesistenza e contaminazione di saperi diversi, per effetto dei quali, in qualunque settore si operi, la competenza specialistica in una data materia, da sola, rischia di non essere più sufficiente. In altre parole, oggi, ma non da oggi, è necessario essere il più possibile aggiornati, o quanto meno informati, sulle principali acquisizioni delle altre discipline scientifiche e, di conseguenza, sarà sempre più frequente l'eventualità che qualunque 'attore' delle indagini e del processo penale si trovi nella necessità di possedere almeno una conoscenza di base delle discipline tecnico-scientifiche nelle quali egli si imbatte.

Occorre, infatti, evitare che lo scienziato o il tecnico abbiano un 'monopolio di conoscenza' che produrrebbe inevitabilmente un potere difficilmente controllabile: quindi, è necessario che ogni attore del processo – non solo il giudice, tradizionalmente definito '*peritus peritorum*' – compia uno sforzo aggiuntivo per avere gli strumenti necessari per controllare il sapere del tecnico.

1 Il G.D.P.R. definisce con l'espressione 'dati biometrici' tutti quei 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.

Ciò, ovviamente, non vuol dire che il giurista debba acquisire un sapere equivalente a quello dell'esperto, quanto invece, se si accetta una metafora forse un po' ardita, che si chiede al giurista, nel valutare un dipinto, non già di essere a sua volta un pittore ma di essere almeno un critico d'arte.

In sintesi, per dirla con le parole del filosofo Isaiah Berlin,[2] bisogna cercare di essere un po' 'ricci' ed un po' 'volpi'.

Questo sintetico contributo, dunque, si dividerà idealmente in due versanti: il primo tenterà di affrontare rapidamente il tema dell'impatto delle tecnologie di riconoscimento automatico del volto nelle indagini preliminari; il secondo si concentrerà sui possibili rischi per la privacy, senza però dimenticare due tra i più importanti profili comuni ad ogni disciplina tecnico-scientifica moderna, vale a dire la sempre crescente importanza delle banche dati alimentate con enormi quantità di informazioni quali i cd. *big data* e lo sviluppo di sistemi di intelligenza artificiale per l'esame di tali dati.

2. L'impatto delle tecnologie di riconoscimento automatico del volto nelle indagini preliminari

È ben noto che una parte assai rilevante degli approfondimenti sul tema dei rapporti fra sapere scientifico e processo penale è avvenuto sulla scia delle elaborazioni dottrinali e giurisprudenziali sviluppate nell'ambito del processo statunitense ed incentrate sul ruolo di '*gatekeeper'* del giudice in quel sistema processuale.[3] Il controllo del giudice,

2 Si fa riferimento al pensiero di Berlin il quale distingueva i pensatori in due categorie: i 'ricci', i quali concentrano i loro sforzi nella perlustrazione di un'area delimitata, e le 'volpi', che preferiscono scorrazzare su un territorio più vasto.

3 Non è neanche ipotizzabile, in questa sede, un tentativo di dare conto dello sterminato dibattito sul tema (per un primissimo approfondimento, si veda https://www.expertinstitute.com/resources/insights/daubert-vs-frye-navigating-the-standards-of-admissibility-for-expert-testimony/) alla luce delle più importanti sentenze della Corte suprema degli Stati Uniti:
sentenza 'Frye' del 1923, secondo la quale il giudice, nel valutare l'ammissibilità di una teoria scientifica nel processo penale, deve accertare che essa sia "*generally accepted as reliable in the relevant scientific community*";
sentenza 'Daubert' del 1993, secondo la quale occorre invece considerare una molteplicità di fattori: 1) se la affidabilità della teoria sia stata testata e stimata; 2) se la teoria sia stata pubblicata e sottoposta al giudizio della

infatti, nel sistema processuale statunitense, si incentra in particolare nella fase della ammissibilità della deposizione di colui che viene definito '*expert witness*'. Per tale ragione, il ruolo del giudice in quel sistema è descritto come *gatekeeper*, espressione che, letteralmente traducibile con 'custode del cancello', potremmo rendere nel contesto che ci riguarda, con 'guardiano dell'accesso'.

Nel sistema processuale italiano, invece, il giudice non è solo un '*gatekeeper*'; egli è soprattutto un fruitore critico del sapere scientifico e, cosa ancora più importante, il giudice italiano è tenuto a motivare le ragioni del proprio convincimento, al contrario di quanto accade nel processo con giuria di ispirazione anglosassone.

Orbene, tutte le discipline tecnico-scientifiche che possono avere un'utilità nel processo penale, ad eccezione degli accertamenti genetici, hanno un tratto che le accomuna: anche a seguito di alcuni casi eclatanti, è stata recentemente posta in dubbio la loro affidabilità ed il loro reale fondamento scientifico sulla base di alcune riflessioni che potrebbero meritare qualche pensiero anche con riguardo al riconoscimento automatico del volto.

Ad esempio, sebbene la tecnica di rilevamento e confronto delle impronte digitali sia universalmente accettata, un noto caso del 2004 – verificatosi in seguito agli attacchi terroristici alla metropolitana di Atocha nella città di Madrid – ha posto seri dubbi sulla solidità della base scientifica su cui si fonda l'identificazione mediante impronte digitali.

Si tratta del noto caso di Brandon Mayfield, avvocato americano che nel 2004 fu tratto in arresto poiché alcune impronte digitali rinvenute sulla scena del crimine degli attacchi terroristici alla metropolitana di Madrid furono a lui erroneamente

comunità scientifica (cd. "*peer review*"); 3) quale sia il tasso di errore della teoria scientifica; 4) l'esistenza di controlli sulla teoria medesima; 5) se la teoria sia "*generally accepted in the scientific community*";
sentenza 'Joiner' del 1997, la quale ha focalizzato la propria attenzione anche sulla metodologia seguita per giungere alle conclusioni e non solo su queste ultime, affermando in particolare che "*conclusions and methodology are not entirely distinct from one another*";
sentenza 'Kumho' del 1999, secondo la quale lo standard 'Daubert' deve trovare applicazione anche alla testimonianza dell'esperto, cd. *expert witness*, che non abbia natura prettamente scientifica ma trovi il proprio fondamento su abilità tecniche o sull'esperienza.

attribuite. Accadde infatti che le immagini di alcune impronte rinvenute su una busta di plastica utilizzata per trasportare una parte del congegno esplosivo utilizzato per l'attentato furono trasmesse dalle autorità spagnole all'FBI. Le immagini furono inserite nel sistema IAFIS (*Integrated Automated Fingerprint Identification System*, Sistema automatico per l'identificazione delle impronte digitali) e si giunse così alla – come detto erronea – identificazione del signor Mayfield. Si scoprì successivamente che Brandon Mayfield non era mai stato in Spagna.[4]

È forse opportuno ricordare che, per quanto eclatante, il caso Mayfield aveva alcune particolarità assai rilevanti, forse decisive: in primo luogo l'attribuzione delle impronte era avvenuta utilizzando immagini di qualità non ottimale e, in secondo luogo, vi erano comunque numerosi punti caratteristici in comune tra le impronte da confrontare.[5]

4 Questo il testo integrale del comunicato stampa emesso dall'FBI dopo la scoperta dell'errore: "After the March terrorist attacks on commuter trains in Madrid, digital images of partial latent fingerprints obtained from plastic bags that contained detonator caps were submitted by Spanish authorities to the FBI for analysis. The submitted images were searched through the Integrated Automated Fingerprint Identification System (IAFIS). An IAFIS search compares an unknown print to a database of millions of known prints. The result of an IAFIS search produces a short list of potential matches. A trained fingerprint examiner then takes the short list of possible matches and performs an examination to determine whether the unknown print matches a known print in the database. Using standard protocols and methodologies, FBI fingerprint examiners determined that the latent fingerprint was of value for identification purposes. This print was subsequently linked to Brandon Mayfield. That association was independently analyzed and the results were confirmed by an outside experienced fingerprint expert. Soon after the submitted fingerprint was associated with Mr. Mayfield, Spanish authorities alerted the FBI to additional information that cast doubt on our findings. As a result, the FBI sent two fingerprint examiners to Madrid, who compared the image the FBI had been provided to the image the Spanish authorities had. Upon review it was determined that the FBI identification was based on an image of substandard quality, which was particularly problematic because of the remarkable number of points of similarity between Mr. Mayfield's prints and the print details in the images submitted to the FBI. The FBI's Latent Fingerprint Unit will be reviewing its current practices and will give consideration to adopting new guidelines for all examiners receiving latent print images when the original evidence is not included. The FBI also plans to ask an international panel of fingerprint experts to review our examination in this case. The FBI apologizes to Mr. Mayfield and his family for the hardships that this matter has caused".

5 "Upon review it was determined that the FBI identification was based on an image of substandard quality, which was particularly problematic be-

Orbene, nella sua indubbia particolarità, il caso Mayfield[6] ci dice che ogni disciplina tecnico-scientifica ha limiti intrinseci e margini di errore che richiedono un approccio prudente e non fideistico, nella consapevolezza che: l'abilità del personale in ogni singola fase del procedimento di esaltazione può essere determinante; esiste il rischio di *bias* cognitivi; l'aspetto delle impronte può essere influenzato da numerosi fattori.[7]

D'altro canto, recenti acquisizioni hanno rivelato che le impronte digitali sono stabili nel tempo[8], come dimostrato da uno studio scientifico che ha tratto origine proprio dalla applicazione pratica dei principi della nota sentenza 'Daubert' pronunciata dalla Corte Suprema degli Stati Uniti nel 1993,[9] secondo la quale tra i vari fattori da considerare prima di accordare l'ingresso nel processo ad una prova scientifica vi è che sia noto il tasso statistico di errore della disciplina considerata. Il tasso statistico di errore, infatti, era noto con riferimento all'unicità delle impronte digitali ma, a causa della mancanza di studi sistematici, non per la loro persistenza nel lungo termine.

Uno studio del 2015 condotto da Soweon Yoon – del *National Institute of Standards and Technology* – e da Anil K. Jain – dell'Università del Michigan – ha mostrato che gli indici di somiglianza fra due impronte prelevate a distanza di tempo diminuiscono leggermente ma consentono una identificazione accurata.[10]

Ecco allora un aspetto cruciale che deve essere tenuto presente sin da ora: le criticità che riguardano le altre tecniche di identificazione potrebbero presentarsi anche per il riconoscimento facciale automatico. A tal proposito si pensi, a titolo esemplificativo, all'impatto delle condizioni di luce,

cause of the remarkable number of points of similarity between Mr. Mayfield's prints and the print details in the images submitted to the FBI".

6 Per una analisi approfondita del caso Mayfield e di molti altri, nonché per riflessioni di carattere generale sulla 'crisi' delle scienze forensi, si suggerisce la lettura del volume *Autopsy of a crime lab* (al momento disponibile in Italia sono in lingua inglese).

7 Superficie di contatto, strisciamento, pressione non uniforme ed etc.

8 Maggiori informazioni a questo link: https://www.lescienze.it/news/2015/07/03/news/impronte_digitali_stabilita_nel_tempo-2677479/.

9 *Supra*, nt. 1.

10 Per eventuali approfondimenti: https://www.pnas.org/doi/10.1073/pnas.1410272112.

alla qualità degli strumenti di ripresa, all'abbigliamento indossato, ecc.

Il riconoscimento del volto può essere definito come 'abilità antropomorfa', nel duplice senso che come ogni altra tecnica di identificazione biometrica, esso si basa su caratteristiche fisiche della persona; tuttavia, a differenza di quasi tutte le altre tecniche biometriche di identificazione – ed analogamente per quanto accade con il riconoscimento vocale –, il riconoscimento del volto ha una corrispondente abilità umana.

L'aspetto di maggior rilievo delle tecnologie di riconoscimento facciale risiede però nella sua estrema potenza perché tale tecnica, a differenza di tutte le altre tecniche biometriche è '*contactless*',[11] può prescindere dalla collaborazione del soggetto e si presta a un utilizzo massivo e occulto.

D'altra parte, è proprio quest'ultima caratteristica delle tecnologie di riconoscimento facciale a fare di esse uno strumento particolarmente potente e utile nella fase delle indagini preliminari, specialmente se applicato alle riprese fotografiche o video effettuate dalla polizia giudiziaria.

Un primo dato interessante, che testimonia la novità dell'argomento, è che non risultano precedenti giurisprudenziali: tutte le sentenze in tema di 'riconoscimento' riguardano il mezzo di prova disciplinato dall'art. 213 c.p.p.[12] oppure il riconoscimento fotografico.[13]

Come deve qualificarsi un sistema di riconoscimento automatico del volto nel processo penale? Ci si trova di fronte ad una prova atipica oppure ad una attività che richiede 'specifiche competenze'? O forse ancora ad un misto delle due cose?

Una cosa pare possa essere affermata con certezza: il principio generale, ai sensi del considerando n. 71[14] del

11 Non richiede il contatto fisico con la persona soggetta ad identificazione.

12 Esso prevede la ricognizione effettuata da un essere umano su persone fisicamente presenti.

13 La giurisprudenza prevalente riconduce tale strumento alla nozione di prova atipica prevista dall'art. 189 c.p.p.

14 "L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani".

G.D.P.R., è che non si dovrebbe subire una decisione basata unicamente su un trattamento automatizzato e dunque senza interventi umani.

Il software attualmente utilizzabile dalle forze dell'ordine italiane è denominato 'S.A.R.I. – Sistema Automatico Riconoscimento Immagini' e, ad oggi, esiste in due versioni, la prima denominata *Enterprise*, e la seconda denominata *Real-Time*.

La prima è attiva dal 2018 e funziona in remoto, vale a dire su immagini già acquisite che vengono confrontate automaticamente con le immagini delle persone 'fotosegnalate' presenti nella banca dati 'A.F.I.S.'; attraverso l'utilizzo di due algoritmi di riconoscimento facciale è in grado di fornire un elenco di immagini ordinato secondo un grado di similarità. La comparazione fisionomica 'definitiva' – nel rispetto della previsione del regolamento G.D.P.R. – viene però effettuata dagli operatori specializzati della Polizia Scientifica.

Per quanto concerne invece la 'SARI *Real-Time*', essa potrebbe funzionare in modo analogo ma, come indica la sua denominazione, è in grado di analizzare in tempo reale i volti individuati da videocamere.

Tuttavia, il secondo sistema analizzato non può essere in concreto utilizzato poiché la sua utilizzazione è stata inibita in forza di un parere del Garante per la protezione dei dati personali del 25 marzo 2021. Tale parere, infatti, dopo una sintetica ma efficace analisi dei punti essenziali del problema, ha fondato la propria decisione sulla ritenuta inesistenza di una adeguata base normativa che consenta il trattamento dei dati.

3. I possibili rischi per la privacy

La vicenda della 'SARI *Real-Time*' è emblematica del tema ricorrente del rapporto tra individuo e autorità, o, per essere più precisi, della individuazione di un punto di equilibrio tra autorità e libertà.

'*Real-time*', infatti, come si è detto, significa che il sistema consente, attraverso una serie di telecamere installate in una data area, di analizzare in tempo reale i volti dei soggetti ripresi e di confrontarli con una banca dati dedicata, la cd. *watchlist*, che contiene al massimo 10.000 volti.

Il citato parere del Garante, come si è detto, si fonda sulla inesistenza di un'adeguata base normativa che consenta il trattamento dei dati in tempo reale.

Si tratta, dunque, di una valutazione che potrebbe essere di segno opposto nel momento in cui dovesse essere introdotta una 'adeguata base normativa' che consenta di utilizzare le tecnologie di riconoscimento automatico del volto ed il trattamento informatizzato dei dati così ottenuti.

Cosa potrebbe accadere se dovesse essere effettivamente introdotta tale 'adeguata base normativa' che consenta l'uso di tali tecnologie?

La risposta, ovviamente, dipenderà in larga misura da come sarà formulata la base normativa.

Si può, tuttavia, tentare di evidenziare sin da ora che tali norme, considerato che sono coinvolti diritti di rilevanza costituzionale, dovranno rispettare i principi di determinatezza, frammentarietà e proporzionalità, che sempre più spesso vengono in gioco quando si tratta, come senza dubbio accade nel caso in esame, di strumenti idonei a comprimere diritti fondamentali.

Una recentissima sentenza della sesta sezione della Corte di cassazione,[15] in tema di dati di traffico telefonico e di geolocalizzazione,[16] mette a fuoco perfettamente la questione enunciando principi teoricamente applicabili ad ogni ipotesi di "strumenti di raccolta automatizzata di dati personali" e dunque anche ai dati ottenuti con le t.r.f.

La base normativa, poi, dovrà necessariamente confrontarsi con alcuni rischi potenziali.

In primo luogo, il fatto che, per funzionare adeguatamente, i sistemi automatici richiedono grandi quantità di dati, i cd. *big data*, nel caso specifico basi di dati alimentate da immagini di volti umani trattate biometricamente, vale a

15 Cass., Sez. VI, 14 aprile 2023, n. 15836.

16 Questa la 'massima': "in tema di acquisizione di dati contenuti in tabulati telefonici, non sono utilizzabili nel giudizio abbreviato i dati di geolocalizzazione relativi a utenze telefoniche o telematiche, contenuti nei tabulati acquisiti dalla polizia giudiziaria in assenza del decreto di autorizzazione dell'autorità giudiziaria, in violazione dell'art. 132, comma 3, d.lgs. 30 giugno 2003, n. 196, in quanto prove lesive del diritto alla segretezza delle comunicazioni costituzionalmente tutelato e, pertanto, affette da inutilizzabilità patologica, non sanata dalla richiesta di definizione del giudizio con le forme del rito alternativo".

dire ricondotte ad una stringa alfanumerica quantificabile e conseguentemente suscettibile di confronto.

Saranno, pertanto, altrettanto necessari sistemi di intelligenza artificiale che consentano di confrontare rapidamente l'immagine ottenuta con quelle, numerosissime, presenti nei database.

Tali sistemi di intelligenza artificiale, a loro volta, fondati sull'utilizzo di software proprietari con algoritmi di cui non è ben noto il funzionamento, potrebbero far sorgere il rischio di trovarsi di fronte ad una '*black box*', vale a dire un sistema di cui sono noti i dati che vengono inseriti – cd. *input* – ed i dati che si ottengono in risposta – cd. *output* – ma non anche i meccanismi di funzionamento.[17]

L'utilizzo su larga scala delle tecnologie di riconoscimento facciale, inoltre, porrebbe seri problemi non ancora del tutto noti al grande pubblico derivanti dalla acquisizione e dal trattamento – specie se unitamente alle numerosissime altre tipologie di dati, biometrici o meno, che ogni persona genera quotidianamente – di dati estremamente sensibili.

Si pensi anche soltanto alla possibilità di ricostruire nel dettaglio e per ciascuna persona, anche da parte di soggetti privati e non necessariamente le cd. *big tech*, le quali, anzi, potrebbero essere frenate dagli 'aspetti reputazionali' e prescindendo dall'esistenza di una indagine penale alcuni aspetti riservati della vita privata di ciascuno, come, ad esempio, le abitudini, le frequentazioni, le partecipazioni a manifestazioni culturali, politiche o sindacali, le attività *online*.[18]

Tale ricostruzione, peraltro, ma pare un dato di particolare rilievo, potrebbe avvenire unitamente ad una geolocalizzazione molto più precisa di quella ottenibile, ad esempio, con la acquisizione dei dati di traffico telefonico o telematico e, allo stato, senza alcun limite temporale per la '*data retention*'.

17 Con la conseguente necessità di introdurre sistemi di *eXplanaible Artificial Intelligence* (XAI), tema immensamente complesso e, ovviamente, non limitato alle tecnologie di riconoscimento facciale.

18 Emblematico il caso di 'Clearview AI', società americana che ha messo in atto un vero e proprio 'monitoraggio biometrico' anche di persone che si trovavano su territorio italiano. Per eventuali approfondimenti, si veda il link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751323.

4. Conclusioni

Il tema, certamente non agevolmente sintetizzabile, è estremamente delicato e complesso e non si presta a rapide semplificazioni.

Si può forse dire, tuttavia, che la diffusione delle tecnologie di riconoscimento facciale – specie se utilizzate in modo complementare alle ormai innumerevoli 'tracce digitali' che ogni essere umano produce e disperde nel mondo moderno – potrebbe contribuire in modo decisivo a svelare anche gli aspetti più intimi della vita privata di ogni persona e quindi a tracciarne un profilo fedelissimo, utilizzabile per gli scopi più diversi.

Parafrasando, molto liberamente, Luigi Pirandello potrebbe dirsi che ci troviamo ai confini di un'epoca, o forse ci siamo già entrati e non ce ne siamo accorti, in cui nessun essere umano potrà realmente scegliere la 'maschera' con la quale mostrarsi perché il suo volto – 'vero' o soltanto ricostruito da un *software* – sarà stato scoperto ed analizzato approfonditamente.

LUCI E OMBRE DELLA PROVA SCIENTIFICA NEL PROCESSO PENALE

Massimo Motisi
Consiglio dell'Ordine degli Avvocati del Foro di Palermo

Abstract: The paper explores the contribution of technical ascertainment in the criminal process, with particular regard to the role of defence.

Parole chiave: prova scientifica; processo penale; diritto di difesa.

1. Premessa

Il tema del presente contributo afferisce all'indiscussa centralità che le scienze forensi – intese quali tecniche e metodologie scientifiche applicate all'amministrazione della giustizia – assumono nei processi penali.

Il noto filosofo e giurista inglese Jeremy Bentham affermava che "i testimoni sono gli occhi e le orecchie della giustizia"[1] e la verità di questa affermazione ha resistito nel tempo, seppur sia evidente come lo spazio processuale occupato dalla prova scientifica stia gradualmente marginalizzando quello della prova dichiarativa.

Invero, è sufficiente volgere il pensiero ai fatti più noti di cronaca nera italiana per comprendere quanto il ricorso alla prova scientifica sia ormai determinante ai fini dell'accertamento della verità processuale in un senso ovvero nell'altro, qualora la stessa, come meglio vedremo, non venga eseguita secondo le previsioni normative.

Certamente, venti o trent'anni fa, le possibilità investigative offerte dall'attuale evoluzione tecnologica e scientifica non erano neppure lontanamente immaginabili; ciò nonostante, il ricorso alla scienza da parte del giudice penale non è una novità e, infatti, nella storia giudiziaria mondiale era frequente che l'organo giudicante attingesse dal sapere scientifico dell'epoca per decidere su un caso. Si pensi al noto 'caso

1 Bentham 1842.

Dreyfus' scoppiato in Francia sul finire del XIX secolo che prese il nome dall'omonimo protagonista, capitano dello Stato maggiore francese, accusato di tradimento e spionaggio a favore della Germania, che venne processato e condannato sulla base di quella che, all'epoca, venne ritenuta una evidenza scientifica. Infatti, nel tentativo di stabilire la paternità del celebre documento incriminato, caduto in mano nemica, l'Accusa francese aveva sottoposto ad interrogatorio alcuni esperti calligrafici, i quali avevano concluso in favore dell'appartenenza dello scritto a Dreyfus, sulla base di un confronto tra lo scritto incriminato e la corrispondenza privata del capitano dal quale erano emerse delle cd. coincidenze. Ebbene, la frequenza statistica di tali coincidenze aveva determinato la condanna, nonostante i giudici avessero ammesso di non avere compreso la *ratio* sottostante le complesse dimostrazioni matematiche esposte dei testimoni.

2. I metodi scientifici maggiormente utilizzati

Oggi – stante il raro ricorso alla scrittura manuale – la perizia calligrafica rientra tra i metodi scientifici meno ricorrenti, al contrario di altri che trovano costantemente spazio in ambito processuale. Si pensi alla cd. genetica forense che spazia dagli accertamenti sul DNA all'analisi tossicologica dei capelli per acclarare un'attribuzione di paternità o la presenza di uno specifico soggetto sulla scena del crimine, ovvero alle nuove frontiere dell'indagine dattiloscopica rappresentata dall'analisi poroscopica avente ad oggetto le particolarità che circoscrivono gli orifizi sudoriferi delle estremità papillari.

È possibile inoltre fare riferimento anche ad altre preziose tecniche investigative: la cd. entomologia forense, avente ad oggetto l'analisi degli insetti sul corpo della vittima al fine di accertarne i tempi della morte; l'antropologia forense, la quale sfrutta strumenti propri degli studi antropologici applicati nel contesto legale al fine del riconoscimento dei resti umani; la balistica forense, necessaria per lo studio dei proiettili e delle loro traiettorie, nonché i materiali impiegati tramite l'uso di armi da fuoco.

Nel corso dei processi si registra sempre più frequentemente il ricorso anche a due ulteriori strumenti investigativi: l'indagine stilometrica ed il sonogramma. La prima si basa sull'accertamento dello stile linguistico di un determinato soggetto attraverso lo studio statistico delle caratteristiche degli stili letterali, delle scelte lessicali, della lunghezza delle parole, delle costruzioni sintattiche e del modo di collegare le parti del discorso; la seconda, invece, consente di misurare la frequenza, la durata e l'intensità di un segnale vocale in raffronto con altro campione vocale.

Nel corso di questa rapida rassegna è doveroso richiamare anche la possibilità di applicare alla sfera giuridica le conoscenze sul nostro cervello – le cd. neuroscienze – al fine di comprenderne struttura e funzioni. Sul punto, un argomento costantemente indagato dal mondo neuroscientifico riguarda la rilevazione dell'impulsività e dell'aggressività di una persona attraverso lo studio del funzionamento alterato del sistema cerebrale della serotonina.

3. Il rapporto tra il mondo scientifico ed il mondo processuale

Come si può intuire, l'attuale competenza delle scienze forensi è vastissima e spazia dalla chimica alla fisica, dalla medicina alla psicologia forense. Tuttavia, la coesione tra i due mondi – quello scientifico e quello processuale – non è immune da problemi.

In via preliminare, si ricorda come non sempre il ricorso alla prova scientifica in ambito processuale rafforzi le certezze, aprendo talvolta la strada a nuove problematiche: si pensi a tutti quei casi in cui la scienza si limita ad offrire dati statistici espressi in forma di leggi probabilistiche sul verificarsi o meno di una certa affermazione.

Per comprendere meglio quanto detto è opportuno prendere come riferimenti l'ambito medico-sanitario ovvero il cd. *criminal profiling*,[2] i quali offrono spunti certamente uti-

2 Tecnica investigativa, messa a punto dagli americani, che ha il compito di fornire agli investigatori informazioni specifiche che facilitino l'identificazione di criminali sconosciuti, riducendo così la serie dei 'sospetti' ad una

li ma con dubbi margini di certezza laddove si consideri che ogni persona ha caratteristiche proprie ed un proprio vissuto che la rendono diversa da ogni altra e potrebbero dunque 'falsare' la ricerca *de qua*.

Così come, sotto altro profilo, va evidenziato come gli interessi processuali contrapposti spingano le parti ad una ricerca che sia 'interessata', ossia chiaramente volta alla scoperta di evidenze favorevoli alla propria tesi ovvero sfavorevoli a quella della controparte, piuttosto che alla ricerca della verità che, come si comprende, nel processo penale raramente si pone in termini di oggettività.

Tanto premesso, il primo e fondamentale problema legato al ricorso agli accertamenti scientifici nel processo penale attiene alla valutazione che il giudicante – non già in sede di valutazione, bensì in fase di ammissione delle prove – è tenuto ad effettuare in ordine alla validità ed affidabilità della prova scientifica, dovendone peraltro darne espressamente conto nella motivazione. La risposta a questo importante quesito si deve alla giurisprudenza statunitense, ed in particolare a due emblematiche sentenze il cui contenuto è stato ampiamente recepito dalla giurisprudenza mondiale, inclusa quella italiana: la sentenza Frye del 1923 e la sentenza Daubert del 1993.

Nel caso '*Frye vs United States*', l'imputato accusato di omicidio aveva chiesto di essere sottoposto al test della macchina della verità al fine di valutare la veridicità delle sue affermazioni misurando le variazioni della pressione arteriosa ad ogni risposta.

All'epoca, la Corte d'Appello del *District of Columbia* si era ritrovata nella situazione di dover valutare l'ammissibilità di uno strumento sino a quel momento mai utilizzato e la cui validità scientifica appariva alquanto discutibile. Pertanto, i giudici si sentirono in dovere di rivolgersi alla comunità scientifica di riferimento cui spettava il potere di decisione e dalla delega agli scienziati era risultata l'inammissibilità del test della macchina della verità perché non sufficientemente accettato dalla comunità scientifica. Dunque, con la 'sentenza Frye' veniva fissato il criterio, che avrebbe dominato la scena giuridica dei settant'anni successivi, secondo cui la prova scientifica am-

serie più o meno ridotta di individui con determinate caratteristiche specifiche.

missibile deve essere ancorata alla generale accettazione da parte della comunità scientifica di riferimento.

Nel successivo 1993, con il caso '*Daubert vs. Merrel Dow Pharmaceuticals*', la Corte Suprema degli Stati Uniti compiva un passo ulteriore: il solo cd. standard Frye circa l'accettazione generale della prova scientifica non era più sufficiente alla valutazione di una prova scientifica incerta.

Invero con il 'caso Daubert', la Corte ha introdotto la possibilità di ammettere una prova sulla base di nuovi principi,[3] oltre al riconoscimento della comunità scientifica, quali: la possibilità di sottoporre la teoria o tecnica scientifica a verifica empirica, falsificarla e confutarla; l'esistenza di una revisione critica da parte degli esperti del settore; l'indicazione del margine di errore noto o potenziale e il rispetto degli standards relativi alla tecnica impiegata.

Ecco che oggi il vaglio di affidabilità del metodo scientifico impone al giudice un duplice onere: per un verso, acquisire gli elementi di valutazione necessari il giudizio sfruttando il contraddittorio fra le parti, il contributo dell'esperto e l'utilizzo dei propri poteri officiosi; per altro verso, motivare adeguatamente sul punto – a pena di nullità della sentenza – confrontandosi con le possibili spiegazioni alternative dell'evento concreto e dimostrando con le sue argomentazioni che l'ipotesi accolta, appaia l'unica plausibile a fronte della inidoneità esplicative delle altre.

Ciò che, invece, il giudice non può e non deve fare è sicuramente trasformarsi da mero fruitore del sapere scientifico in scienziato in tutti quei casi in cui vi sia un contrasto fra più tesi controverse; egli non può schierarsi a favore di una di esse, senza dar conto delle fonti e delle opinioni degli esperti dalle quali ha tratto il suo convincimento ovvero omettendo di incaricare un perito quando occorra accertare un determinato fenomeno scientifico, procedendo lui stesso, secondo propri indimostrati parametri valutativi.

3 In Italia i principi in questione sono stati recepiti successivamente con la famosa sentenza Cozzini del 2010.

4. Accertamenti tecnico-scientifici nel codice di procedura penale

Fatte queste doverose premesse in ordine alla natura della prova scientifica ed alla necessità di una sua 'validazione' ai fini del suo utilizzo, si pone il problema delle modalità tramite le quali la stessa debba fare materialmente ingresso all'interno del meccanismo processuale.

Com'è noto, il catalogo dei mezzi di prova offerti dal nostro codice non è un numero chiuso ed invero, l'art. 189 c.p.p. permette alle indagini scientifiche di trovare accoglimento in ambito processuale nelle forme più diverse purché nel rispetto dei limiti a garanzia della cd. legalità probatoria. Quest'ultima prevede che non si tratti di prove vietate dalla legge o manifestamente superflue o irrilevanti e che si tratti di prove idonee ad assicurare l'accertamento dei fatti e che le stesse non pregiudichino la libertà morale della persona.

Quanto alla disciplina riservata agli strumenti di indagine scientifica, il codice offre svariati riferimenti diretti.

Nella disciplina della fase delle indagini preliminari si fa riferimento ai cd. accertamenti e rilievi, cui il codice non attribuisce alcuna definizione, la quale risulta invece essere stata elaborata dalla giurisprudenza: mentre i rilievi implicherebbero un'attività di mera osservazione, individuazione ed acquisizione di dati materiali,[4] gli accertamenti comporterebbero un'opera di studio critico, di elaborazione valutativa e di giudizio dei dati precedentemente 'rilevati'.[5]

Sul punto, nel nostro sistema processuale è pacifico che in fase di indagine sia la polizia giudiziaria sia le difese delle parti possano autonomamente compiere rilievi ed accertamenti ripetibili – per tali intendendosi tutte quelle attività che consentono di cristallizzare, senza alterazioni, le tracce, i reperti lo stato dei luoghi e sono prodromici al successivo intervento del pubblico ministero – i cui esiti confluiranno direttamente nel fascicolo del pubblico ministero ovvero

4 Si pensi all'individuazione di un'impronta dattiloscopica o delle tracce di residui del processo di esplosione di un'arma da sparo.

5 Si pensi alla comparazione tra l'impronta raccolta e l'impronta di soggetti sospettati ovvero le prove ematiche effettuate in ospedale per accertare lo stato di ebbrezza o, ancora, le prove effettuate mediante analisi delle urine per verificare la previa assunzione di sostante stupefacenti.

in quello del difensore e, salvo un accordo acquisitivo, non potranno essere utilizzati in dibattimento[6] se non eventualmente attraverso l'audizione quale teste del consulente.

Più controverso invece è il tema relativo all'effettuazione dei cd. accertamenti tecnici irripetibili, ossia tali da cagionare la distruzione o la irreversibile alterazione del reperto. In questo caso, infatti, la disciplina è molto più rigida al fine di garantire la formazione della prova in contraddittorio tra le parti.

Posto che il legislatore non ha provveduto ad individuare gli atti non ripetibili né ad indicare i criteri necessari per qualificare tale un atto del procedimento, secondo un criterio generale 'la non ripetibilità' è strettamente ricollegata all'inevitabile modificazione di cose, di luoghi e di persone e spetta all'interprete stabilire quali atti rientrino o meno nella categoria. Non vi è dubbio, ad esempio, che l'autopsia su un cadavere rientri tra gli accertamenti tecnici irripetibili venendo eseguita nell'immediatezza del decesso.

Allo stesso modo può considerarsi irripetibile la verifica del tasso alcolemico eseguita sul conducente autore di un reato stradale.

Tuttavia, mentre in alcuni casi l'irripetibilità di un accertamento è indubbia, vi sono tipologie di accertamento la cui natura – di atto ripetibile o irripetibile – è stata ampiamente dibattuta. A titolo esemplificativo, generalmente si ritiene che l'analisi spettroscopica sulle particelle di polvere da sparo prelevate a mezzo del cd. *stub* sia un accertamento tecnico ripetibile e, dunque, per la sua esecuzione nel corso delle indagini preliminari non debba essere previamente avvisato il difensore dell'indagato, così come i suoi risultati possono essere utilizzati ai fini dell'adozione di un provvedimento cautelare, ancorché acquisiti senza contraddittorio con la difesa.

Tuttavia, spesso, in casi giudiziari di una certa rilevanza a livello nazionale, i risultati forniti dalle analisi sui residui dello sparo sono oggetto di contestazione stanti le modalità con cui sono stati eseguiti i relativi prelievi, posto che le attività preparatorie del campione possono comportare l'alterazione o la contaminazione del campione da esaminare e, quindi, condizionare l'esito finale degli accertamenti.

6 Ad eccezione dell'eventuale ricorso ad uno dei riti alternativi previsti nel nostro ordinamento giuridico cd. allo stato degli atti.

O ancora, tra i dibattiti più accesi vi è quello sulla ripetibilità o irripetibilità degli accertamenti tecnici in ambito informatico.

Uno dei punti su cui ci si interroga con maggiore frequenza attiene al rischio che, durante le operazioni volte a recuperare e conservare gli elementi di prova digitale, ne vengano compromesse genuinità e integrità, con la conseguente dispersione e inutilizzabilità del risultato così ottenuto.

Così come, sul punto, devono citarsi gli accertamenti sul DNA e, invero, se astrattamente l'accertamento tecnico sui campioni genetici potrebbe considerarsi un atto ripetibile: in realtà lo si considera irripetibile qualora l'acquisizione dei campioni genetici sia avvenuta con metodi 'eterodossi', con tutte le conseguenze che ciò comporta in tema di nullità / inutilizzabilità.

5. Problemi processuali degli accertamenti tecnici

Ebbene, posta la necessità di verificare caso per caso la natura degli accertamenti tecnico-scientifici al fine di stabilire quale sia il regime di volta in volta applicabile, occorre brevemente enucleare le problematiche più comuni sottese all'ingresso dei già menzionati accertamenti nella macchina processuale.

Un primo problema riguarda il cd. omesso avviso del compimento degli accertamenti irripetibili, essendo assai frequenti le ipotesi in cui il pubblico ministero compia accertamenti irripetibili *ex* art. 360 c.p.p. senza darne previo avviso all'indagato ed al suo difensore.

Nel caso dell'omessa notifica *de qua*,[7] il codice prescrive una nullità a regime intermedio rilevabile anche d'ufficio, ma non oltre la sentenza di primo grado, ovvero – se la stessa si è verificata nel corso del giudizio – dopo la sentenza di grado successivo da cui deriva la totale inutilizzabilità dei relativi atti, che, peraltro, non è affrancabile mediante l'esame testimoniale del consulente tecnico.[8]

7 Secondo giurisprudenza ormai consolidata la notifica deve essere effettuata non soltanto nei confronti del soggetto formalmente indagato, ma anche in favore di chi, pur non essendo formalmente iscritto nel registro delle notizie di reato, sia già stato raggiunto da indizi di reità.

8 Ad eccezione del caso in cui l'imputato abbia avanzato richiesta di giudizio abbreviato, richiedendo un giudizio allo stato degli atti.

Specularmente, laddove il difensore svolga investigazioni difensive nella fase delle indagini preliminari, lo stesso non potrà compiere accertamenti tecnici che importino una modificazione irreversibile dello stato dei luoghi, tale da rendere l'accertamento stesso non ripetibile.

Un secondo problema attiene alla necessità o meno di procedere secondo le forme di cui all'art. 360 c.p.p., anche nell'ipotesi di cd. rilievi irripetibili[9] a seguito dell'emergenza di nuove circostanze che ne suggeriscano l'opportunità.

Per chiarire meglio la difficoltà in questione si pensi all'ipotesi in cui la polizia giudiziaria, una volta esaurita l'attività di sopralluogo ed a seguito dell'assunzione della direzione delle indagini da parte del pubblico ministero, ritenga di volere effettuare nuovi rilievi su luoghi o cose già oggetto di sequestro.[10]

Secondo la giurisprudenza consolidata della Suprema Corte, sembrerebbe che i già menzionati rilievi – ancorché irripetibili – possano essere effettuati senza la necessità di avvisare preventivamente le parti.

Peraltro, l'orientamento in parola sembrerebbe confermato anche dalla disciplina legislativa elaborata in tema di investigazioni difensive *ex* art. 391 *decies* c.p.p., laddove si stabilisce che se il difensore deve procedere ad accertamenti tecnici non ripetibili, deve darne avviso, senza ritardo, al pubblico ministero; al contrario, nel caso in cui debba compiere altri atti non ripetibili 'di cui al comma 2' – ossia gli atti non ripetibili compiuti in occasione dell'accesso ai luoghi e, tra questi, i rilievi irripetibili – dovrà darne avviso al pubblico ministero il quale, personalmente o mediante delega alla polizia giudiziaria, ha soltanto una facoltà di assistervi, senza poter quindi nominare un proprio consulente che partecipi alle operazioni, e senza poter sollevare riserva di promuovere incidente probatorio.

Ciò suggerisce che, specularmente, il pubblico ministero possa compiere rilievi irripetibili senza dover rispettare le garanzie di cui all'art. 360 c.p.p.

9 Si ricorda che si tratta di un'ipotesi distinta e separata da quella relativa agli accertamenti tecnici.

10 Si pensi al rilievo di impronte dattiloscopiche o di tracce del DNA su beni rinvenuti sulla scena del delitto.

Altra dibattuta questione attiene alla possibilità che gli accertamenti tecnici irripetibili di competenza del pubblico ministero possano essere delegati alla polizia giudiziaria ovvero se nell'ipotesi *de qua* il pubblico ministero debba necessariamente conferire un incarico ad un consulente tecnico, così come previsto letteralmente dall'art. 360 c.p.p.

In realtà, la giurisprudenza maggioritaria sembrerebbe orientata a 'salvare' gli accertamenti tecnici irripetibili eseguiti dalla polizia giudiziaria anche in assenza di conferimento di incarico ad un consulente, purché gli stessi siano accompagnati dagli avvisi e dalle garanzie prescritti dalla più volte menzionata norma.

Tuttavia, ci si domanda come possa essere assicurato il rispetto del contraddittorio qualora il pubblico ministero deleghi il compimento degli accertamenti tecnici alla polizia giudiziaria.

La soluzione che ormai nella prassi viene adottata dalle procure è quella di richiedere il rispetto delle garanzie di cui all'art. 360 c.p.p. – si pensi all'effettuazione degli avvisi di rito alle parti –, quale espressione del principio generale del contraddittorio *ex* art. 111 Cost.

Infine, l'ultima problematica che appare opportuno analizzare in questa sede si verifica nell'ipotesi in cui la polizia giudiziaria compia rilievi irripetibili in caso di urgenza *ex* art. 354 c.p.p., senza dare avviso all'indagato della sua facoltà di farsi assistere dal difensore.

L'art. 356 c.p.p. attribuisce al difensore dell'indagato la facoltà di assisterlo per il compimento degli atti di cui all'art. 354 c.p.p., senza tuttavia prevedere alcun diritto di preavviso; specularmente, l'art. 114 disp. att. c.p.p. prevede che la polizia giudiziaria, nel procedere al compimento degli atti indicati nell'art. 356 c.p.p., deve avvertire l'indagato che ha la facoltà di farsi assistere dal difensore di fiducia. In ogni caso l'inizio delle operazioni non è necessariamente subordinato all'arrivo del difensore.

La violazione della disposizione che presidia l'assistenza dell'indagato al compimento dell'atto, rientra tra le nullità a regime intermedio verificatasi nella fase delle indagini, e può essere dunque rilevata od eccepita prima della deliberazione della sentenza di primo grado.

6. Riflessioni conclusive

A conclusione di questo approfondimento relativo alle principali problematiche sottese all'ingresso della prova scientifica nella macchina processuale, si ritiene doveroso un breve richiamo agli accertamenti cd. invasivi / coattivi, intendendosi con tale espressione quegli accertamenti che possono essere eseguiti anche contro la volontà dell'interessato.

È noto come per anni gli accertamenti coattivi venissero eseguiti vincendo l'eventuale contraria volontà del soggetto passivo, grazie ad un inciso dell'art. 224 c.p.p. che consente al giudice di adottare "tutti gli altri provvedimenti che si rendono necessari per l'esecuzione delle operazioni peritali".

Ciò sino al 1996, allorquando la Corte costituzionale – chiamata a pronunciarsi su un caso di prelievo ematico coattivo – pur riconoscendo che il prelievo ematico costituisse una "pratica medica di ordinaria amministrazione", per la prima volta ha affermato come lo stesso comportava "certamente una restrizione della libertà personale quando se ne renda necessaria l'esecuzione coattiva perché la persona sottoposta all'esame peritale non acconsente spontaneamente al prelievo".

Muovendo da questo rilievo, la Consulta ha ritenuto illegittimo l'art. 224 comma 2 c.p.p., "nella parte in cui consente che il giudice, nell'ambito delle operazioni peritali, disponga misure che comunque incidano sulla libertà personale senza determinare la tipologia delle misure esperibili e senza precisare i casi ed i modi in cui esse possono essere adottate", di fatto anticipando ciò che il legislatore avrebbe introdotto soltanto nel 2009 con la previsione dell'art. 224-*bis* c.p.p. che, com'è noto, stabilisce i casi di ammissibilità degli accertamenti coattivi e le forme del relativo provvedimento autorizzativo.

È evidente come all'indomani della richiamata sentenza della Corte costituzionale, la distinzione tra prelievi invasivi e non invasivi abbia assunto importanza decisiva.

Invero, posto che è generalmente qualificabile come 'prelievo' qualsiasi manovra diretta a raccogliere materiale biologico necessario per l'esecuzione di ricerche ed analisi, lo stesso si reputa invasivo ogniqualvolta il suo svolgimento implichi il superamento del limite fisico dell'individuo e incida sulla sua integrità fisica.

Sul punto, gli inglesi hanno ulteriormente marcato la distinzione tra 'prelievi non intimi'[11] e 'prelievi intimi'[12] stabilendo che si considerano espressamente non invasivi della sfera corporale i seguenti elementi: i prelievi di unghie, capelli, ed altre parti esterne non sensibili del corpo, gli accertamenti medici diversi dalle ispezioni personali che non richiedono la somministrazione di sostanze o l'introduzione di strumenti nel corpo della persona sottoposta all'esame e la raccolta di materiale biologico che avrebbe comunque abbandonato la sfera fisica della persona.

Al fine di colmare la lacuna formatasi nel nostro ordinamento a seguito della citata sentenza della Corte costituzionale, il legislatore italiano è intervenuto inizialmente nel 2005 attraverso l'aggiunta del comma 2-*bis* all'art. 349 c.p.p., il quale consente alla polizia giudiziaria di procedere al prelievo coattivo di capelli o saliva a soli fini identificativi.

Interventi successivi si sono registrati con l'adesione dell'Italia al Trattato di Prum, e con l'introduzione degli articoli 224-*bis* e 359-*bis* nel codice di procedura penale.

Ebbene, posto che nessun problema si pone quando l'interessato presta il consenso al prelievo, il richiamato art. 224-*bis* c.p.p. ammette l'ipotesi di prelievo coattivo del DNA purché vengano rispettati dei limiti a pena di inutilizzabilità dell'accertamenti. Le limitazioni in questione possono essere circoscritte in: edittali – si tratta di operazioni consentite solo in ordine a delitti dolosi o preterintenzionali puniti con ergastolo o detenzione superiore a 3 anni –, di necessarietà, poiché il prelievo deve essere "assolutamente indispensabile per la prova dei fatti" ovvero di forma, in quanto l'ordinanza con cui dispone accertamento coattivo deve contenere una serie di avvisi e deve essere regolarmente notificata all'interessato dal difensore.

Da ultimo, si prevede che l'individuo non possa comunque consentire ad atti che comportino una diminuzione permanente dell'integrità fisica o psichica o che ledano la propria dignità personale.

Per concludere il presente contributo, è evidente come l'esponenziale progressione che le scienze forensi hanno

11 Capelli, peli non pubici, unghia.

12 Sperma, urina, saliva, peli pubici e impronte dentali.

avuto negli ultimi decenni abbia notevolmente influenzato lo svolgimento dei processi penali, contribuendo a ridurre il margine di potenziali errori giudiziari.

Da qui sorge la necessità di ribadire l'importanza del ruolo dello scienziato che, al pari di quello del giudice e dei difensori – intesi tutti come 'celebranti' del processo – implica un'enorme responsabilità nei confronti dell'attività che è chiamato a svolgere.

Invero, richiamando la nota metafora di Calamandrei "non dobbiamo dimenticarci mai che tutte le nostre simmetrie sistematiche, tutte le nostre *elegantiae juris*, diventano schemi illusori se non ci avvediamo che al di sotto di essi, di vero e di vivo non ci sono che gli uomini, colle loro luci e le loro ombre, con le loro virtù e le loro abberazioni".

Bibliografia

Bentham 1842: Bentham G., *Teoria delle prove giudiziarie*, Bruxelles, 1842.

Editorial and publishing policies

Publishing proposals are to be submitted to the Director of the *History, Law & Legal History* series (director.hllh@unipa.it).

One or two Reviewers will evaluate each proposal by means of a double-blind peer-review process. If a revision of the work is requested, the Referees will ascertain if the Author has made the requested changes. If there are inconsistencies with the latter, the work will be submitted to the Scientific Board for a final evaluation.

On submission of their work, the Authors will declare that it is an original piece of work, which does not breach intellectual property or other rights. The Authors must also ensure that their book or chapter does not contain any libellous matter or violate any copyright or other intellectual property rights. The Authors are obliged to cite content from other appropriate sources in order to avoid plagiarism.

The Reviewers will behave in a fair and impartial manner; they will review the material in a timely manner and assist in improving the quality of a submitted proposal or typescript by reviewing the material with care, consideration and objectivity. The Reviewers will inform the Editorial board of any published or submitted content, which is similar to the material under review, or of any suspected plagiarism; they will also maintain the confidentiality of any information or material submitted during the review process.

The Director will: act in a fair and balanced way when carrying out their duties; devoid of discrimination; manage submissions in a timely manner; and treat all material as confidential. They will also provide guidance to the Authors regarding the expectations of the publication and the decision-making process regarding which books to publish, in turn is based on the quality and suitability for the said series.

HISTORY, LAW & LEGAL HISTORY

1. Raimondo Santoro, *Per la storia dell'*obligatio *I.*, 2020.
2. Mario Varvaro (a cura di), *L'eredità di Salvatore Riccobono*, 2020.
3. Antonio Lindiner, *Credito immobiliare ai consumatori e obblighi di condotta degli intermediari*, 2021.
4. Ulrico Agnati and Mario Varvaro (eds.), *Religion, Ideology, Politics, and Law. A Multidisciplinary Approach in the Frame of European History*, 2022.
5. Anna Maria Giomaro e Maria Luisa Biccari, *Sulle* regulae iuris *fra I e III secolo: Paolo commenta Plauzio*, 2022.
6. Ornella Spataro, *Sindacato di legittimità costituzionale e legalità penale. Il delicato equilibrio tra ruolo della Corte costituzionale e discrezionalità del legislatore negli itinerari giurisprudenziali più recenti*, 2022.
7. Vincenzo Roberto Imperia, *I vescovati nella Sicilia normanna (secc. XI-XII). Potestà normative e competenze giurisdizionali in un territorio multiculturale*, 2022.
8. Annarosa Gallo, Maria Colomba Perchinunno, Michele Dionigi e Pierangelo Buongiorno (a cura di), *Ordinamento giuridico, mondo universitario e scienza antichistica di fronte alla normativa razziale (1938-1945)*, 2022.
9. Caterina Scaccianoce, *Prova tecnica e contraddittorio nel processo penale*, 2023.
10. Simona Feci, *I criminalisti dello Stato della Chiesa. Famiglie, carriere e biblioteche (XVII secolo)*, 2023.
11. Stefania Pietrini, *La legislazione di Zenone (474-491)*, 2023.
12. Caterina Ventimiglia, *Amministrazione performante e sistema dei controlli interni*, 2023.
13. Mario Varvaro (ed.), *Human Rights Reloaded*, 2024.
14. Lorenzo Acconciamessa, *Principi costituzionali fondamentali ed esclusione dell'illecito internazionale*, 2024.
15. Giuseppe Lauricella (a cura di), *Questioni istituzionali nel dibattito attuale*, 2024.
16. Monica De Simone, *Forme di appartenenza alla comunità politica romana. Dalla nascita di Roma alla fine del Principato*, 2024.
17. Paola Di Simone, Annalisa Mangiaracina e Lucia Parlato (a cura di), *120 anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, 2024.

Finito di stampare nel mese di
dicembre 2024
presso
Fotograph s.r.l.
Palermo

Editing e typesetting
Michela D'Alessandro
per conto di NDF

Il volume raccoglie gli atti del Convegno tenutosi a Palermo nell'aprile del 2023, presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Palermo, nella ricorrenza dei centoventi anni dalla fondazione della Polizia Scientifica italiana. In questa occasione professionisti della Polizia scientifica, magistrati, avvocati e docenti universitari si sono confrontati con una materia di crescente rilievo, ossia l'identificazione personale, per offrire una riflessione alla comunità di studiosi e operatori.

La discussione ha ripercorso così la lunga evoluzione che ha portato la Polizia Scientifica a utilizzare tecniche investigative sempre più avanzate. Se in passato la 'traccia' che conduceva al 'criminale' era costituita per lo più dalle impronte digitali, oggi l'apporto della scienza all'interno del procedimento penale si avvale di nuovi strumenti. Il loro impatto sui diritti fondamentali delle persone indagate o imputate e di soggetti 'terzi', come evidenziato da esperti del settore, si è posto al centro di complesse valutazioni e delicati bilanciamenti. All'approfondimento relativo alla prova del DNA nel processo penale si è accompagnato quello sul riconoscimento facciale che, nelle sue molteplici configurazioni, si basa su procedure bisognose di regolamentazione normativa ed è oggetto di attenzione anche da parte della Corte di Strasburgo.

HISTORY
LAW &
LEGAL
HISTORY