Memorie del Dipartimento di Giurisprudenza
dell'Università degli Studi di Torino

Ernestina Sacchetto

Tecnologie di riconoscimento facciale e procedimento penale

Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna

UNIVERSITÀ DI TORINO
Dipartimento di Giurisprudenza
Giappichelli

Memorie del Dipartimento di Giurisprudenza dell'Università degli Studi di Torino

7

Comitato scientifico:

Valeria Marcenò (*coordinatrice*)
Alessandra Algostino
Stefano Barbati
Roberto Cavallo Perin
Maurizio Cavanna
Federico Consulich
Elena D'Alessandro
Riccardo de Caria
Paolo Gallo
Michele Graziadei
Enrico Grosso
Daniela Izzi
Barbara Lavarini
Anna Mastromarino
Pier Giuseppe Monateri
Simona Novaretti
Michele Rosboch
Michele Vellano
Annamaria Viterbo
Georgia Zara
Ilaria Zuanazzi

IUSTITIAM COLIMUS

Ernestina Sacchetto

Tecnologie di riconoscimento facciale e procedimento penale

Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna

UNIVERSITÀ DI TORINO
Dipartimento di Giurisprudenza
Giappichelli

© Copyright 2025 – G. Giappichelli Editore - Torino
10124 Torino, Via Po, 21 - Tel. 011-81.53.111
http://www.giappichelli.it

ISBN/EAN 979-12-211-1517-8
ISBN/EAN 979-12-211-8182-1 (ebook)

© Copyright 2025 – Università degli Studi di Torino
10124 Torino, Via Verdi 8
www.collane.unito.it/oa/
www.openaccess@unito.it

ISBN/EAN 978-88-759-0351-0

Il presente volume è stato preliminarmente sottoposto a un processo di referaggio anonimo, nel rispetto dell'anonimato sia dell'Autore sia dei revisori (double blind peer review)*.*
La valutazione è stata affidata a esperti del tema trattato, nominati dal Comitato Scientifico della Collana in conformità al Regolamento delle pubblicazioni del Dipartimento di Giurisprudenza dell'Università di Torino. I revisori hanno formulato un giudizio positivo sull'opportunità di pubblicare il presente volume.

Opera finanziata con il contributo del Dipartimento di Giurisprudenza dell'Università di Torino.

G. Giappichelli Editore

Questo libro è stato stampato su carta certificata, riciclabile al 100%

Stampa: Stampatre s.r.l. - Torino

Quest'opera è distribuita con Licenza Creative Commons Attribuzione - Non commerciale Non opere derivate 4.0 Internazionale

Le fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume/fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941, n. 633.

Le fotocopie effettuate per finalità di carattere professionale, economico o commerciale o comunque per uso diverso da quello personale possono essere effettuate a seguito di specifica autorizzazione rilasciata da CLEARedi, Centro Licenze e Autorizzazioni per le Riproduzioni Editoriali, Corso di Porta Romana 108, 20122 Milano, e-mail autorizzazioni@clearedi.org e sito web www.clearedi.org.

Alla mia famiglia

Indice

pag.

Abbreviazioni XIII

Introduzione XV

Capitolo I
Le tecnologie di riconoscimento facciale prima e oltre il processo penale

1. L'inarrestabile diffusione della tecnologia di riconoscimento facciale 1
2. Le "comunità intelligenti" fanno fronte all'insicurezza urbana 8
3. La corsa alla regolamentazione 15

Capitolo II
Inquadramento tecnico-scientifico e funzionamento operativo degli strumenti

1. Il percorso di analisi 21
2. *βίος* e *μέτρον*: una ricostruzione semantica della categoria di riferimento 22
   2.1. Il dato biometrico nel recente quadro normativo 32
3. Le proprietà dei tratti biometrici e le classificazioni dei sistemi di riconoscimento 40
4. Il funzionamento tecnico della tecnologia di riconoscimento facciale 46
   4.1. Le peculiarità del Sistema Automatico di Riconoscimento delle Immagini (SARI): contesto di riferimento e dettagli operativi 53

pag.

4.2. La banca dati AFIS – SSA 56
4.3. Tecniche di intelligenza artificiale e riconoscimento facciale 62
4.4. Il calcolo del rapporto di verosimiglianza nella scienza forense 67
4.5. Le finalità di verifica, identificazione e categorizzazione biometrica 69
4.5.1. Il riconoscimento delle emozioni 72
4.6. Livello di accuratezza e tipologie di errore nella tecnologia di riconoscimento facciale 74
5. Il ruolo assunto dalle informazioni biometriche e le categorie di riferimento 78

Capitolo III
L'impatto trasversale sui diritti fondamentali

1. La tecnologia di riconoscimento facciale e le garanzie processuali coinvolte 83
2. Il riconoscimento facciale automatizzato e la libertà personale 86
3. Nuovi e più labili confini tra gli artt. 13 e 24 Cost.: il *nemo tenetur se detegere* nel quadro delle nuove intrusioni nella sfera personale 92
4. Il trattamento del dato biometrico digitalizzato nel rispetto del diritto alla riservatezza 98
4.1. Un'ipotesi specifica di trattamento: il processo decisionale automatizzato 108
4.2. Il perimetro del trattamento tra i principi di limitazione della finalità e di minimizzazione dei dati 111
4.3. Approcci giurisprudenziali stranieri all'impatto del riconoscimento facciale sul diritto alla riservatezza: il procedimento inglese *Ed Bridges (R)* c. *The Chief Constable of South Wales Police* 119
4.4. (*Segue*) L'affaire *Glukhin* c. *Russia*: prime indicazioni da Strasburgo 127
5. I rischi per la parità delle armi 136
5.1. I sistemi di intelligenza artificiale tra trasparenza e spiegabilità dei risultati: i rimedi tecnici indispensabili al diritto di difesa e al contraddittorio 141

pag.

5.2. Tra interpretabilità e certificazione del metodo 145
5.3. I criteri di equità e di legalità 147

Capitolo IV
Tentativi di regolamentazione fra normativa interna e sovranazionale

1. Considerazioni introduttive 151
2. L'esperienza italiana e il SARI 154
2.1. Il decreto "capienze" e l'inerzia del legislatore 158
3. Il quadro normativo sovranazionale: verso un sistema armonizzato di regole 163
3.1. Dal Libro bianco della Commissione europea alla Convenzione sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto nell'ambito del Consiglio d'Europa 168
3.2. Il regolamento europeo sull'intelligenza artificiale 171
3.2.1. I sistemi di riconoscimento biometrico a distanza: per la prima volta uno schema normativo di riferimento 178
3.2.2. Gli strumenti di riconoscimento *in tempo reale* 181
3.2.3. Gli strumenti di riconoscimento *a posteriori* 190
3.2.4. Alcune prime brevi riflessioni sul regolamento 193
4. Le ricadute sulla cooperazione di polizia e gli sviluppi del sistema di scambio e di circolazione dei dati 195

Capitolo V
La comparazione automatizzata fra volti nell'attuale assetto codicistico

1. Alla ricerca delle adeguate coordinate processuali 203
2. L'acquisizione dei volti a fini di comparazione 207
3. La rappresentazione digitalizzata del volto entro il *genus* della "prova digitale" 216
4. La modalità applicativa *a posteriori*: nuovo trattamento o nuovo metodo? 223

pag.

4.1. Il riconoscimento *a posteriori* e la categoria della prova atipica 228
4.1.1. Il requisito della libertà morale 232
5. La modalità applicativa *in tempo reale* 234
6. La capacità dimostrativa di un *match* biometrico 248
6.1. L'attendibilità del *match* biometrico 252
6.1.1. Il ruolo del calcolo del rapporto di verosimiglianza 255

Capitolo VI
Riflessioni e prospettive *de iure condendo*

1. Osservazioni conclusive. Da dove veniamo? Chi siamo? Dove andiamo? 261
2. Gli standard tecnici comuni tra certezza del diritto e innovazione tecnologica 266
3. Le modalità *in tempo reale* e *a posteriori* entro il sistema codicistico in una prospettiva *de iure condendo* 270

Bibliografia essenziale 277

Abbreviazioni

1:1 – One-to-One Matching
1:N; 1:N+1 – One-to-Many Matching
AFIS – Automated Fingerprint Identification System
AFRL – Automated Facial Recognition Locate
APIS – Automated Palmprint Identification System
AI ACT – Artificial Intelligence Act (reg. UE 2024/1689)
ANN – Artificial Neural Network
CBR – Case-based reasoning
CCTV – Closed Circuit Television
CDFUE – Carta dei diritti fondamentali dell'Unione europea
CGUE – Corte di giustizia dell'Unione europea
C. eur. – Corte europea dei diritti dell'uomo
Conv. eur. dir. uomo – Convenzione europea dei diritti dell'uomo
DNA – Acido desossiribonucleico (*DeoxyriboNucleic Acid*)
EDPB – European Data Protection Board
EDPS – European Data Protection Supervisor
EDRi – European Digital Rights
ENFSI – European Network of Forensic Science Institutes
FAR – False Acceptance Rate
FISWG – Facial Identification Scientific Working Group
FRR – False Rejection Rate
GDPR – General Data Protection Regulation
Ge.F.I. – Genetisti Forensi Italiani
IA – Intelligenza Artificiale
IBG – International Biometric Group
ICT – Internet communication technology
IoT – Internet of Things
ISFG – International Society for Forensic Genetics
IT – Information Technology
LED – Law Enforcement Directive
LLM – Large Language Model
LR – Likelihood Ratio
ML – Machine Learning

NFI – Netherland Forensic Institute
NIST – National Institute of Standards and Technology
NLP – Natural Language Processing
NSTC – National Standard Technology Council
NU – Nazioni Unite
OCSE – Organizzazione per la cooperazione e lo sviluppo economico
OECD – Organizzazione per la Cooperazione e per lo Sviluppo Economico
RBR – Rule-based reasoning
SARI – Sistema Automatico Riconoscimento Immagini
SSA – Sottosistema Anagrafico
TULPS – Testo Unico delle Leggi di Pubblica Sicurezza
UIDAI – Unique Identification Authority of India
XAI – Explainable Artificial Intelligence

Introduzione

La ricerca che qui si comincia affronta un tema già emerso nel dibattito pubblico, ma sinora non ancora approfondito in ambito processuale penale, concernente l'impiego delle tecniche di riconoscimento facciale tramite software, divenute negli ultimi anni particolarmente utili per facilitare alcuni passaggi cruciali nell'*iter* di identificazione.

Al fine di orientare l'approccio del lettore e prevenire possibili fraintendimenti circa le aspettative di una trattazione immediatamente ancorata alle tradizionali categorie processuali, si rendono opportune due premesse di ordine metodologico e sistematico. In primo luogo, occorre chiarire che la tematica oggetto di studio non si esaurisce in una trattazione unitaria e circoscritta, ma affiora progressivamente seguendo una linea direttrice che attraversa trasversalmente l'intero sviluppo dell'elaborato. Pertanto, taluni profili strettamente processuali, per la necessità di essere pienamente compresi alla luce delle premesse e dei presupposti teorico-normativi illustrati nei capitoli iniziali, richiedono di essere affrontati necessariamente nelle fasi più avanzate del lavoro.

In secondo luogo, si anticipa che la complessità del tema in esame – per sua natura intersettoriale e tecnicamente connotato – impone un approccio volto ad adattare le tradizionali categorie probatorie alle nuove esigenze poste dall'impiego di tecnologie digitali. Lungi dal costituire un esercizio meramente esegetico, tale operazione mira a valorizzare, in chiave euristica, il potenziale evolutivo degli istituti tradizionali, affinché possano fungere da strumenti di qualificazione giuridica di prassi emergenti che sollevano interrogativi centrali per la riflessione sul processo penale come luogo di razionalità giuridica, equilibrio tra poteri e tutela dei diritti fondamentali.

Per tale ragione, lo studio non può che partire da una ricostruzione delle attuali applicazioni e da una descrizione tecnica del funzionamento degli strumenti di riconoscimento in esame. Le definizioni di base e l'analisi dei fondamenti della disciplina biometrica saranno utili per comprendere e analizzare le peculiarità delle più specifiche tecniche di riconoscimento facciale, sia rispetto al tratto del volto in sé considerato, sia con riferimento al "*biometric match*", scaturente dalla comparazione automatizzata eseguita tramite

software [1]. Ciò in ragione del fatto che la conoscenza degli elementi fondamentali di una disciplina (anche piuttosto complessa, come in questo caso) è necessaria al fine di prevenire semplificazioni inopportune e conclusioni affrettate.

Non saranno, invece, oggetto di analisi, se non per una breve descrizione [2], i sistemi di riconoscimento delle emozioni, finalizzati ad associare in via automatizzata uno stato d'animo o un comportamento non verbale, sulla base delle contrazioni muscolari del volto. Sebbene la tecnologia alla base del funzionamento di questi software sfrutti una delle più tradizionali finalità applicative dei sistemi di riconoscimento biometrico (la categorizzazione) [3], il tema meriterebbe una trattazione a sé stante che farebbe necessariamente sviare l'indagine verso complessi dibattiti sull'impiego di dispositivi tecnologici e di controllo dell'attendibilità dei contributi dichiarativi quali, ad esempio, l'ipnosi, la narcoanalisi, il poligrafo e la risonanza magnetica.

Si intende qui, invece, concentrare l'attenzione sulla finalità di riconoscimento fisionomica, esaminandone le implicazioni giuridiche e metodologiche nell'ambito dell'identificazione biometrica, senza estendere la trattazione a questioni che attengono alla verifica, all'autenticazione, o alla categorizzazione dei tratti e della veridicità delle dichiarazioni mediante tecnologie di monitoraggio neurofisiologico e psicofisiologico [4]. Pertanto, al fine di far emergere sin da subito l'urgenza di una trattazione sistematica a fini processuali, l'analisi si aprirà con l'inquadramento del tema, mettendone in luce la rilevanza assunta in vari settori. Saranno analizzate le prime applicazioni del riconoscimento facciale in contesti extra-procedimentali, per delineare il quadro evolutivo della tecnologia e il suo progressivo inserimento nei meccanismi di accertamento processuale. Si passerà poi ad una breve ricostruzione dei più rilevanti progetti nazionali di sorveglianza urbana, con i casi-pilota di Como, Torino, Venezia e Trento, seguendo un percorso evolutivo che condurrà al primo quadro normativo in materia, a livello nazionale, per poi concludersi con un riferimento al recente regolamento europeo sull'intelligenza artificiale. A questo punto, si concentrerà l'attenzione sul funzionamento di questi strumenti e sulla relativa terminologia non sempre d'uso comune, attingendo alla letteratura informatica e indagando le varie

[1] Cfr. il capitolo II, § 3.

[2] Cfr. il capitolo II, § 3.5.1.

[3] Cfr. il capitolo II, § 3.5.

[4] Per un approfondimento si rinvia al capitolo II, §§ 3.5 e 3.5.1.

fasi che interessano il procedimento di riconoscimento biometrico, nonché le sue principali finalità applicative. L'impiego di tecniche di intelligenza artificiale costituisce un livello di complessità ulteriore per la materia, configurandosi al contempo come un passaggio ormai imprescindibile nell'analisi dei processi automatizzati applicati al riconoscimento biometrico. In effetti, il trattamento della rappresentazione digitalizzata di un volto, in assenza dell'implementazione di tali metodologie, risulta di per sé privo di un'effettiva rilevanza operativa e scientifica, rendendo dunque necessario un approfondimento sulle modalità di elaborazione e interpretazione dei dati biometrici mediante sistemi di apprendimento automatico e reti neurali. Comprendere e risalire all'architettura e al funzionamento di questi strumenti può risultare un'operazione estremamente complessa, se non addirittura impossibile, con evidenti potenziali ricadute su molteplici diritti fondamentali e garanzie processuali poste a presidio dell'individuo.

In tale contesto, sarà condotta un'analisi delle diverse tipologie di errore che possono insorgere nell'impiego della tecnologia di riconoscimento facciale, nonché delle circostanze in cui tali sistemi possono risultare alterati, o meno accurati, a causa di inevitabili distorsioni sistemiche. Tali fenomeni, potenzialmente forieri di esiti discriminatori nei confronti dei soggetti sottoposti a identificazione automatizzata, impongono una riflessione critica sulla loro compatibilità con i principi fondamentali dell'ordinamento giuridico. A questo proposito, al fine di valutare l'adeguatezza del quadro normativo vigente, gli sforzi successivi saranno tesi a illustrare i diritti fondamentali potenzialmente compromessi dall'impiego delle tecnologie di riconoscimento facciale, con particolare riferimento alla libertà personale, alla tutela della riservatezza e al principio di parità delle armi.

Indagati i rischi derivanti dal ricorso a questi strumenti, il capitolo successivo approfondirà le disposizioni previste dal quadro normativo italiano recentemente introdotto, analizzandone il contenuto alla luce dei provvedimenti dell'Autorità Garante per la protezione dei dati personali.

È nel contesto dell'Unione europea, però, che la tecnologia di riconoscimento facciale ha ricevuto, per la prima volta, un inquadramento giuridico sistematico, volto a disciplinarne in maniera organica l'impiego, con particolare riferimento ai sistemi di riconoscimento biometrico a distanza. L'intervento regolatorio dell'Unione europea ha segnato una svolta epocale nel tentativo di colmare il vuoto normativo che, per diverso tempo, aveva caratterizzato l'utilizzo di tali strumenti, introducendo un *corpus* di disposizioni finalizzato a bilanciare le esigenze di sicurezza pubblica e prevenzione dei reati con la salvaguardia dei diritti fondamentali della persona, nella

consapevolezza delle implicazioni invasive che derivano dall'impiego di tecnologie idonee a rilevare, analizzare e trattare dati biometrici in modalità non cooperativa e su larga scala. Con l'adozione del regolamento (UE) 2024/1689 sull'intelligenza artificiale, è stata introdotta una disciplina che stabilisce criteri e limiti per l'utilizzo di tali tecnologie, prevedendo una fase di implementazione e di adozione da parte degli Stati membri nei mesi successivi alla sua entrata in vigore.

Prima di indagare le modalità attraverso le quali il legislatore nazionale dovrebbe recepire e attuare le disposizioni del regolamento, si renderà necessario verificare l'adeguatezza e la tenuta delle tradizionali categorie processuali a fronte delle varie finalità che questi strumenti possono raggiungere all'interno del procedimento. L'analisi seguirà il *ciclo della prova biometrica digitale*, dalla fase di acquisizione del dato grezzo fino alla produzione del *match*, nel tentativo di collocare tali dinamiche entro le categorie probatorie esistenti.

In conclusione, si proporrà uno sguardo alle prospettive future, attraverso due principali filoni di indagine. Da un lato, si valuterà la possibilità di una progressiva espansione dell'impiego del riconoscimento facciale automatizzato, come peraltro sembrano suggerire i più recenti interventi normativi; dall'altro, si esamineranno le modalità attraverso le quali il diritto è chiamato a regolamentarne l'applicazione, individuando le sfide giuridiche emergenti e le soluzioni normative necessarie per bilanciare l'innovazione tecnologica con la tutela dei diritti fondamentali.

Capitolo I
Le tecnologie di riconoscimento facciale prima e oltre il processo penale

SOMMARIO: 1. L'inarrestabile diffusione della tecnologia di riconoscimento facciale. – 2. Le "comunità intelligenti" fanno fronte all'insicurezza urbana. – 3. La corsa alla regolamentazione.

1. *L'inarrestabile diffusione della tecnologia di riconoscimento facciale*

Un sistema di riconoscimento facciale *automatizzato* [1] può essere definito come la tecnologia in grado di riconoscere, con un certo grado di probabilità, una persona da un'immagine digitale o da un fotogramma ripreso da una sorgente video [2].

---

[1] È opportuno precisare preliminarmente che il termine *automatico* designa un sistema intrinsecamente autonomo, in grado di operare senza necessità di intervento umano, eseguendo un'azione predefinita. Al contrario, l'aggettivo *automatizzato* si riferisce a un processo originariamente manuale, trasformato in automatico mediante l'impiego di strumenti informatici, algoritmi o metodologie finalizzate alla riduzione o all'eliminazione dell'intervento umano. Tale distinzione è cruciale nell'ambito dell'architettura di un sistema, in quanto evidenzia la differenza tra strumenti nativamente autonomi e processi che hanno subito una transizione tecnologica per conseguire un funzionamento indipendente. Allo stato attuale, la tecnologia di riconoscimento facciale può operare in modo *automatico* nella fase di rilevamento e identificazione di un volto, eseguendo tali operazioni senza necessità di intervento umano grazie all'impiego di algoritmi avanzati di elaborazione delle immagini. Tuttavia, il successivo processo di analisi e risposta può essere *automatizzato*, ovvero strutturato mediante strumenti informatici che consentono la gestione, l'archiviazione e la catalogazione delle immagini in modo sistematico e continuo, riducendo al minimo la necessità di supervisione umana e ottimizzando l'efficienza operativa del sistema. Per un approfondimento cfr. G.A. MAGNANI-G. FERRETTI-P. ROCCO, *Tecnologie dei sistemi di controllo*, McGraw-Hill, New York, 2011.

[2] *Gruppo di lavoro "Articolo 29", parere 2/2012 – WP 192, relativo al riconoscimento facciale nell'ambito dei servizi online e mobili*, adottato il 22 marzo 2012. Più ampiamente cfr. il capitolo II, § 2.

Il funzionamento di questi strumenti trae fondamento dalla disciplina biometrica avente ad oggetto l'analisi dei parametri biofisici, fisiologici e comportamentali, nonché delle modalità attraverso cui tali caratteristiche vengono rilevate, elaborate e confrontate[3]. Tramite tali informazioni è possibile distinguere un soggetto da un altro in base a caratteristiche come le impronte digitali, il DNA, la forma dell'iride, la struttura vascolare della retina, la configurazione venosa della mano, oppure attraverso i tratti differenziali del comportamento, come il modo di camminare o il timbro della voce.

I sistemi automatizzati di riconoscimento facciale, come si vedrà più dettagliatamente in seguito, si caratterizzano per un peculiare vantaggio operativo, ossia l'assenza di qualsivoglia necessità di collaborazione attiva da parte del soggetto sottoposto alla rilevazione. La tecnologia, infatti, si fonda sull'acquisizione di immagini del volto in modo non interattivo, risultando indifferente a modificazioni comportamentali, volontarie o meno, poste in essere dal destinatario della misurazione. Tale autonomia funzionale consente di effettuare l'operazione di riconoscimento a distanza in assenza di un consenso da parte dell'interessato, rendendo possibile il rilevamento facciale automatico in forma tendenzialmente occulta, senza alcuna manifestazione esterna di volontà o percezione dell'atto da parte del soggetto.

L'ampia diffusione di contenuti visivi attraverso piattaforme online, pagine web personali e *social network* ha reso le rappresentazioni digitalizzate dei volti sempre più accessibili, ampliando significativamente il bacino di dati a disposizione per l'elaborazione e l'impiego di sistemi di riconoscimento facciale. A ciò si aggiunge la crescente disponibilità di ulteriori fonti per l'acquisizione di immagini biometriche, tra cui la capillare rete di telecamere di videosorveglianza, sia fisse che mobili, dislocate sul territorio per finalità di pubblica sicurezza. Tale contesto ha favorito lo sviluppo di infrastrutture tecnologiche in grado di analizzare e processare *in tempo reale* un elevato numero di dati biometrici, sollevando al contempo alcuni interrogativi cruciali in merito alla compatibilità di tali strumenti con i principi posti a protezione dei dati personali e di tutela della riservatezza[4].

Inoltre, questa tecnologia si distingue rispetto alla generalità dei sistemi di identificazione biometrica per un livello di accessibilità in continuo aumento, determinato da diversi fattori convergenti. In primo luogo, la progressiva riduzione dei costi di sviluppo e di implementazione degli strumenti

[3] Cfr. il capitolo II, § 3.

[4] Cfr. il capitolo III.

ha reso i sistemi di riconoscimento sempre più sostenibili dal punto di vista economico, favorendone l'adozione da parte di un numero crescente di attori, sia pubblici che privati. Parallelamente, il costante miglioramento delle prestazioni, dovuto all'evoluzione dei modelli di intelligenza artificiale e all'aumento della potenza computazionale[5], ha determinato un incremento dell'efficienza operativa di tali strumenti, riducendo i tempi di elaborazione e aumentando l'accuratezza dei riconoscimenti. Per tale ragione, i sistemi di riconoscimento facciale sono stati integrati in diversi dispositivi, telecamere a circuito chiuso o *smartphone*, rendendo sempre più agevole la verifica e la raccolta delle immagini ivi registrate.

Tale scenario ha contribuito alla "normalizzazione" del ricorso a questa tecnologia, con effetti rilevanti tanto sotto il profilo socio-culturale, quanto sotto quello giuridico.

In ambito pubblico, l'impiego dei sistemi di riconoscimento facciale da parte delle forze di polizia ha gradualmente acquisito centralità quale strumento di ausilio per le attività investigative, agevolando l'identificazione di soggetti, il rintraccio di persone scomparse e il supporto nell'espletamento di funzioni di controllo alle frontiere. In quest'ultimo contesto, la tecnologia è stata altresì adoperata nell'ambito della gestione delle politiche migratorie e dei procedimenti di rimpatrio, fungendo da strumento di monitoraggio dei soggetti sottoposti a provvedimenti amministrativi o giurisdizionali[6].

L'adozione di tali tecnologie si è estesa anche in altri ambiti del settore amministrativo, dove si è assistito all'emergere di applicazioni peculiari, tra cui spicca, per la portata e la rilevanza, il controverso progetto *Aadhaar*, sviluppato in India, avente l'obiettivo di ottimizzare l'erogazione di sussidi, benefici economici, sovvenzioni e servizi pubblici[7]. Ogni soggetto viene

---

[5] Cfr. il capitolo II, § 4.3.

[6] Cfr. N. VAVOULA, *Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism*, in *European Journal of Migration and Law*, 23(4), 2021, p. 457-484; F. PALMIOTTO, *Procedural fairness in automated asylum procedures: Fundamental rights for fundamental challenges*, in *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 55, 2024, 106065, p. 1-10; ID., *Climbing a Wall: Strategic Litigation Against Automated Systems in Migration and Asylum*, in *German Law Journal*, Vol. 25, Special Issue 6, *Strategic Litigation in EU Law*, 2024, p. 935-955; ID., *The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation*, in *EJRR*, 2025, p. 1-24.

[7] Cfr. P. DIXON, *A Failure to "Do No Harm". India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in *Health Technol.*, 7, 2017, p. 539-567.

iscritto al sistema attraverso la rilevazione di dati biometrici (impronte digitali, scansione dell'iride e fotografia del volto) cui viene associato un codice numerico personale, non riassegnabile, composto da dodici cifre, il cosiddetto *Aadhaar number.* La gestione e il trattamento dei dati sono poi affidati a un'autorità indipendente appositamente istituita, la *Unique Identification Authority of India* (UIDAI), la quale svolge funzioni di supervisione e implementazione operativa dell'intero progetto, delineando le procedure tecniche, le modalità di accesso e condivisione dei dati, nonché i protocolli di sicurezza per la conservazione e l'utilizzo delle informazioni personali [8].

Ancora, il riconoscimento automatizzato è stato integrato nei cd. "sistemi di credito sociale", finalizzati ad assegnare un punteggio di affidabilità (cd. *scoring*) ai cittadini sulla base dei comportamenti individuali, valutati tramite l'interconnessione tra dati biometrici e informazioni personali [9]. In tale contesto, la tecnologia ha assunto un ruolo centrale quale strumento di monitoraggio costante, volto a facilitare il controllo sociale attraverso meccanismi premiali o sanzionatori, incardinati in un sistema automatizzato di valutazione [10]. Non di rado, questi strumenti sono stati impiegati per finalità ulteriori rispetto a quelle dichiarate, ad esempio per l'identificazione sistematica di oppositori politici, nonché per il tracciamento e la marginalizzazione di minoranze etniche o religiose [11].

Anche nel settore privato, tali tecnologie possono essere impiegate per finalità di sicurezza, ad esempio, all'interno di esercizi commerciali, istituti

---

[8] Per un approfondimento cfr. S.S. BANERJEE, *Aadhaar: Digital Inclusion and Public Services in India*, in *WDR, Background paper digital dividends*, 2016; D. SADHYA-T. SAHU, *A critical survey of the security and privacy aspects of the Aadhaar framework*, in *Comp. & Sec.*, 140, 2024.

[9] In ambito europeo, la pratica è stata oggetto di un espresso divieto da parte dell'art. 5, par. 1, lett. c del regolamento (UE) 2024/1689 sull'intelligenza artificiale, PE/24/2024/REV/1.

[10] Cfr. R. CREEMERS, *China's Social Credit System: An Evolving Practice of Control*, in *SSRN*, 9 maggio 2018, p. 1-32 e F. LIANG-V. DAS-N. KOSTYUK-M.M. HUSSAIN, *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, in *Pol. and Int.*, 4(10), 2018, p. 415 ss.

[11] Il governo cinese ricorrerebbe alle tecnologie di riconoscimento facciale per eseguire attività di profilazione etnico-razziale nei confronti degli Uiguri, minoranza turcofona e di fede islamica. Cfr. https://www.il-sole24ore.com/art/come-cina-usa-l-intelligenza-artificiale-controllare-uiguri-ABhvE8oB. Per una ricognizione cfr. S. DEL GATTO, *La governance delle nuove tecnologie tra tentativi di regolazione e istanze di self regulation. Il caso del riconoscimento facciale*, in *Riv. it. dir. pubbl. com.*, 2023, p. 42 ss.

bancari, compagnie assicurative, ecc. [12]. Le tecniche di riconoscimento automatico sono già state impiegate all'interno degli stadi, al fine di rendere più efficiente l'accesso alle strutture, durante i concerti, in occasione di manifestazioni pubbliche e addirittura all'interno dei luoghi di culto [13].

Tramite la registrazione e la comparazione del proprio volto è oggi possibile anche eseguire delle transazioni, ovvero personalizzare l'offerta di acquisto per diverse categorie di clienti tramite pubblicità mirate [14]. Nell'ambito della domotica, poi, tali software trovano applicazione per l'accesso alle abitazioni, per il riconoscimento delle persone al loro interno e l'interazione con i dispositivi elettronici.

È dunque agevole constatare l'intensificarsi di una connessione strutturale tra l'impiego dei sistemi di riconoscimento facciale e l'ambito della sicurezza pubblica, in ragione delle crescenti potenzialità e delle molteplici applicazioni che tali tecnologie offrono anche nel settore privato. In particolare, si osserva una progressiva ibridazione funzionale tra i domini pubblico e privato, con la conseguenza che le autorità inquirenti e i soggetti preposti alla tutela dell'ordine pubblico si rivolgono con sempre maggiore frequenza a fornitori di servizi digitali, intermediari tecnologici e piattaforme online, al fine di acquisire dati biometrici e informazioni personali ritenuti rilevanti ai fini delle indagini o delle attività di prevenzione.

Del resto, la sorveglianza e il continuo monitoraggio dei soggetti incarnano una delle più vive manifestazioni autoritative, particolarmente desiderabile agli occhi del potere pubblico anche in quanto dotata di significativa attitudine disciplinante rispetto alle condotte sociali del soggetto passivo del monitoraggio [15]. Il pericolo però è quello di legittimare squilibri nell'assetto

---

[12] Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, p. 19 e E. ROWE, *Regulating Facial Recognition Technology in the Private Sector*, in *Stanf. Tech. Law Rev.*, 24(1), 2021.

[13] Cfr. B. HUTCHINS-M. ANDREJEVCIC, *Olympian Surveillance: Sports Stadiums and the Normalization of Biometric Monitoring*, in *Int. Journ. of Comm.*, 15(2021), p. 363-382; O.H. LENGKONG-S.W. TAJU-C.F. MAABUAT-R.J. JANIS, *Security System To Prevent Terrorism Actions Using Face Recognition In Worship Building, 2023 5th International Conference on Cybernetics and Intelligent System* (ICORIS), 2023, p. 1-6.

[14] Cfr. M. TASPINAR-A.T. NASKALI-G. EREN-M. KURT, *The importance of customized advertisement delivery using 3D tracking and facial recognition*, in *2012 Second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP)*, 2012, p. 520-524.

[15] Cfr. D. GRAY, *The Fourth Amendment in Age of Surveillance*, Editore, Cambridge-New York, 2017, p. 10.

dei rapporti tra poteri e facoltà istituzionali e libertà fondamentali, queste ultime spesso sacrificate sull'altare di esigenze repressive dichiarate impellenti. Si pensi al dibattito suscitato dal noto caso *Clearview AI, start-up* di New York, che ha sviluppato un sistema di riconoscimento facciale, venduto a diverse agenzie di pubblica sicurezza negli Stati Uniti e impiegato per riconoscere gli individui attraverso la comparazione di foto segnaletiche in possesso delle forze di polizia o di fotografie presenti negli archivi delle motorizzazioni civili e pubblicate nelle piattaforme online [16].

Oltre ai potenziali abusi di questa tecnologia, occorre considerare la sempre più diffusa produzione e successiva diffusione di immagini e di video *deepfake* che includono la manipolazione di attributi facciali (*face attribute manipulation*), attraverso cui vengono modificate certe caratteristiche riferibili al volto della persona ritratta (per esempio, invecchiamento o ringiovanimento del viso); le tecniche di scambio dei volti (*face swap*), attraverso le quali, al dato originale presente nell'immagine o video se ne sostituisce un altro (tecnica, peraltro, frequentemente utilizzata per la realizzazione di *deepfake* a sfondo sessuale); le tecniche di *face reenactment* e *lip synching,* attraverso le quali un video viene manipolato in modo tale da modificare i movimenti e le espressioni del volto della persona ritratta, al fine di far sembrare che esse abbiano reso determinate dichiarazioni [17].

A fronte dei possibili rischi derivanti da simili applicazioni, alcuni Stati

---

[16] Cfr. I. NERONI REZENDE, *Facial recognition in police hands: Assessing the "Clearview case" from a European perspective*, in *NJECL*, 11(3), 2020, p. 375 ss.; J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del Garante Privacy D'Oltremanica)*, in *Sist. pen.*, 28 marzo 2020, p. 5; Z.A. KHAN-A. RIZVI, *AI based facial recognition technology and criminal justice: issues and challenges*, in *Turkish Journal of Computer and Mathematics Education*, 12(14), 2021, p. 3384-3392 e J. SCIPIONE-M. LO MONACO, *Has the horse bolted? Dealing with legal and practical challenges of facial recognition*, in *Media Laws*, 18 gennaio 2022. Di recente il Garante per la protezione dei dati personali ha imposto una sanzione di 20 milioni di euro alla società americana *Clearview AI*, per aver posto in essere un vero e proprio monitoraggio biometrico di persone che si trovano nel territorio italiano. Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani*, 9 marzo 2022.

[17] Per un approfondimento sul tema dei *deepfakes*, cfr. *ex multis* G. TESSITORE, *Riconoscimento automatico del volto e confronto in ambito forense*, in P. DI SIMONE-A. MANGIARACINA-L. PARLATO, *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, Palermo University Press, Palermo, 2023, p. 73 ss.; EUROPOL, *Facing reality? Law enforcement and the challenge of deepfakes*, 13 marzo 2024; INTERPOL, *Beyond illusions. Unmasking the threat of synthetic media for law enforcement*, 2024.

oltreoceano, ove sistemi di sorveglianza sono particolarmente diffusi ormai da anni, stanno discutendo dell'opportunità di proibirne determinati impieghi [18]. Anche diverse aziende private hanno manifestato l'intenzione di non sviluppare più tali sistemi di riconoscimento, ovvero di non metterli più a disposizione delle forze di polizia [19].

Si sono sviluppate, dunque, nell'ambito del dibattito scientifico e istituzionale, due principali direttrici interpretative. La prima, di segno più radicale, propone il divieto integrale dell'utilizzo di tali strumenti, ritenendo che le insuperabili problematiche connesse alla protezione dei diritti fondamentali – in particolare alla tutela della riservatezza e della libertà personale – nonché le ricorrenti disfunzionalità sul piano tecnico, impongano un impedimento assoluto del loro impiego, tanto in ambito pubblico, quanto privato.

Una seconda posizione, più moderata, suggerisce invece l'adozione di un approccio regolatorio stringente, volto a consentire l'utilizzazione della tecnologia entro un perimetro giuridico ben definito e coerente con i principi fondamentali dell'ordinamento. Tale impostazione si fonda sull'esigenza di massimizzare i benefici operativi derivanti dall'applicazione dei sistemi di riconoscimento facciale, garantendo al contempo che il loro impiego avvenga possibilmente in condizioni giuridicamente ed eticamente sostenibili.

Al momento, nessun legislatore nazionale dell'area europea ha ancora espressamente raccolto la sfida di stabilire a quali specifiche condizioni e con quali modalità tecniche sia possibile impiegare la tecnologia di riconoscimento facciale con uno "*human centred approach*" [20], mancando una normativa che si riferisca a queste tecnologie con le suddette caratteristiche. Come si vedrà meglio in seguito, l'adozione del regolamento (UE) 2024/1689 sull'intelligenza artificiale rappresenta un primo tentativo di colmare questo vuoto normativo, delineando un quadro di principi

---

[18] Cfr. J. SPIVACK-C. GARVIE, *A Taxonomy of Legislative Approaches to Face Recognition in the United States*, in A. KAK (a cura di), *Regulating Biometrics: Global Approaches and Urgent Questions*, AI Now Institute, New York, 2020, p. 89 ss.

[19] G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 22, precisa che «la statunitense *Axon*, ovvero la più grande produttrice al mondo di videocamere indossabili (c.d. *bodycam*), ha deciso di sospendere le forniture alle forze dell'ordine, ed anche *Big Tech* come *Amazon, Microsoft* e *IBM* hanno annunciato una moratoria o di volere uscire dal mercato delle TRF».

[20] Cfr. il capitolo IV, § 1.

generali che gli Stati membri saranno chiamati a recepire e attuare a livello nazionale [21].

L'Italia, sull'onda del fiorire di progetti finalizzati a incrementare la sicurezza urbana da parte di alcuni Comuni, ha introdotto un primo schema di norme che, però, non definisce specificamente la cornice dei casi e delle condizioni per il ricorso a questa tecnologia [22].

Anche la riflessione giuridica sul punto deve ancora svilupparsi appieno, rimanendo ancora in parte inesplorate le questioni problematiche che originano dall'impiego di questi strumenti, a partire dal loro impatto sui diritti fondamentali e dalla pretesa regolativa che il diritto è chiamato ad avanzare. In questo senso, il diritto processuale penale offre un punto di vista privilegiato per indagare la correlazione che intercorre tra le tecnologie di riconoscimento facciale, la tutela delle libertà fondamentali e l'ambizione del diritto a offrire una disciplina per tali strumenti.

2. *Le "comunità intelligenti" fanno fronte all'insicurezza urbana*

L'urgenza di proporre un inquadramento sistematico del riconoscimento facciale nell'ambito del procedimento penale nasce dal ruolo sempre meno marginale da questo assunto nel settore della sicurezza urbana, a livello nazionale ed europeo [23]. Il profondo interesse che le autorità di pubblica sicurezza e le amministrazioni hanno cominciato a nutrire nei confronti di queste tecnologie e delle società private produttrici dei software è stato ampiamente dimostrato dai diversi progetti di monitoraggio delle aree urbane, introdotti di recente da alcuni Comuni del nord-Italia.

---

[21] Cfr. il capitolo IV, § 3.2.

[22] Cfr. il capitolo IV, § 2.1.

[23] Il concetto di "sicurezza urbana" viene definito dall'art. 4 del d.l. n. 14/2017, conv. con modificazioni dalla legge n. 48/2017, come: «bene pubblico che afferisce alla vivibilità e al decoro delle città, da perseguire anche attraverso interventi di riqualificazione e recupero delle aree o dei siti più degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio, la promozione del rispetto della legalità e l'affermazione di più elevati livelli di coesione sociale e convivenza civile, cui concorrono prioritariamente, anche con interventi integrati, lo Stato, le Regioni e le Province autonome di Trento e di Bolzano e gli enti locali, nel rispetto delle rispettive competenze e funzioni».

Negli ultimi anni, è emersa una stretta correlazione tra la sicurezza dell'ambiente cittadino e l'impiego di tecnologie IT[24] da parte delle autorità di *law enforcement*, considerato come antidoto necessario per affrontare, a livello locale, le sfide per uno sviluppo sicuro e sostenibile[25]. Il concetto di *smart city*[26], pertanto, è sempre con maggiore enfasi indicato come una possibile soluzione alle problematiche di sicurezza, derivanti dall'irreversibile processo di agglomerazione urbana. Questa tendenza è stata attuata, a livello nazionale, con un ampliamento di poteri delle Regioni e, a livello locale, con un crescente coinvolgimento delle forze di polizia nelle attività di controllo urbano del territorio.

A tal proposito, risultano di particolare interesse alcuni casi-pilota di sperimentazione di tecniche avanzate di videosorveglianza, utili per comprendere non solo la particolare rilevanza assunta dalle tecnologie oggetto

---

[24] Con "tecnologia dell'informazione", il cui acronimo è IT (in inglese *Information Technology*), ci si riferisce ai sistemi digitali impiegati allo scopo di memorizzare, modificare e recuperare dati. L'abbreviazione *ICT* invece viene utilizzata per indicare l'impiego della tecnologia nello spazio delle telecomunicazioni (in inglese *Information Communication Technology*).

[25] È possibile riconoscere l'inizio di questo processo in Italia intorno al 2012, quando con il d.l. n. 179/2012 (convertito in legge n. 221/2012) veniva definito un nuovo modello di *governance* diretto a facilitare ed accelerare il processo di realizzazione di *smart cities* e *communities*, sotto la responsabilità e la guida dell'Agenzia per l'Italia digitale (AgID), incaricata di definire le strategie e predisporre gli strumenti per lo sviluppo delle "comunità intelligenti" (che si richiamano nel titolo del paragrafo).

[26] Sebbene non vi sia una definizione unanime del concetto di *smart city*, con tale espressione generalmente si intende un'area urbana in cui le reti e i servizi tradizionali sono resi più efficienti attraverso l'uso di tecnologie digitali e di telecomunicazioni. Tali sviluppi si traducono, ad esempio, in sistemi di trasporto urbano più efficienti e intelligenti, in una gestione ottimizzata delle risorse idriche e delle infrastrutture per lo smaltimento dei rifiuti, nonché in soluzioni tecnologicamente avanzate per l'illuminazione e il riscaldamento degli edifici. Parallelamente, si assiste a una maggiore interattività nell'amministrazione pubblica e a un rafforzamento delle misure volte a garantire la sicurezza degli spazi urbani. Per un approfondimento sul tema cfr. R. FERRARA, *The Smart City and the Green Economy in Europe: a Critical Approach*, in *Energies*, 8, 2015, p. 4724 ss. e C. COLAPIETRO, *Intelligenza artificiale e smart cities: a mò di introduzione*, in M. GIANNELLI-V. PAGNATELLI (a cura di), *Smart cities. Diritti, liberta e governance*, Giappichelli, Torino, 2023, p. XIX. In linea generale, l'espressione si riferisce alle città che impiegano «*new technologies, such as AI and big data analytics, for various applications, such as transportation, trash collection, street repairs, administrative efficiency, surveillance, and more*». M. ZIOSI-B. HEWITT-P. JUNEJA-M. TADDEO-L. FLORIDI, *Smart Cities: Mapping their Ethical Implications*, 5 gennaio 2022 e R. KITCHIN, *The real-time city? Big data and smart urbanism*, in *GeoJournal*, 79, 2014, p. 1-14.

di analisi, ma anche i potenziali e successivi impieghi che i dati raccolti potrebbero avere in un'ottica di prevenzione e repressione dei reati [27].

Il primo caso riguarda il Comune di Como che aveva inserito l'impiego di sistemi di videosorveglianza integrati con la tecnologia di riconoscimento facciale tra le iniziative politiche di sicurezza urbana [28]. Il Comune, infatti, aveva predisposto siffatte misure in base alla normativa che consente l'impiego di impianti di videosorveglianza nel contesto cittadino [29]. Tuttavia, lo stesso quadro di norme non autorizza specificamente il trattamento di dati biometrici [30], come invece richiesto dalla normativa vigente [31]. Non essendo stata

---

[27] Cfr. il capitolo II, § 5.

[28] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 26 febbraio 2020, n. 54.* Cfr. L. CARRER, *Black Box. Sicurezza e sorveglianza nelle nostre città*, Ledizioni, Milano, 2023, p. 101 ss.

[29] Cfr. la legge 23 aprile 2009 n. 38, art. 6, commi 7 e 8, sulla utilizzabilità, da parte dei Comuni, di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana. Cfr. COMUNE DI COMO, *Documento unico programmatico 2020-2022*, reperibile su https://www.comune.como.it/export/sites/default/it/comune/bilanci-documenti-piani/documento-unico-programmazione/DUP-2020-2022.pdf in cui, *inter alia*, si programmava «la "*remise-en-forme*" dell'attuale sistema di videosorveglianza comunale, prevedendo, tra l'altro, una più efficace sistemazione della sala operativa della Polizia Locale [e] (…) una postazione di controllo remoto del sistema di videosorveglianza comunale. Si individueranno in accordo con la PL nuove aree sensibili da sottoporre al controllo di videocamere. La zona dei giardini di viale Tokamachi sarà interessata da un "progetto pilota" per la sperimentazione di funzioni innovative di videosorveglianza, quali *face recognition, loitering*, e rilevamento automatico abbandono/furto di oggetti. La sperimentazione comporta anche la definizione dei rapporti con le altre forze di polizia sia in termini di protocolli di utilizzo che di accesso tecnologico al sistema, nonché, ovviamente, la definizione delle regole di utilizzo conformi al GDPR».

[30] Le disposizioni normative richiamate dal Comune di Como «si limitano infatti, in particolare, a consentire l'identificazione dell'indagato e delle persone in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti (art. 349 c.p.p.), a indicare le modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia (d.P.R. n. 15/2018), ovvero a legittimare l'installazione di videocamere per fini di tutela della sicurezza urbana e comunque in assenza della specifica previsione normativa della raccolta di dati biometrici (art. 6, comma 7, d.l. n. 11/2009), necessaria ai sensi dell'art. 7 d.lgs. n. 51/2018». GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 26 febbraio 2020*, n. 54, cit.

[31] Si veda, in particolare, l'art. 7 del d.lgs. n. 51/2018. Il d.lgs. attua la direttiva 2016/680/UE (cd. LED) del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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

rintracciata alcuna base normativa idonea a giustificare il trattamento dei dati e l'impiego di questa tecnologia, l'Autorità nazionale Garante per la protezione dei dati personali [32], ai sensi dell'art. 37, comma 3, lett. d), del d.lgs. 51 del 2018, ha inibito al Comune la possibilità di continuare a impiegare tale specifica modalità applicativa.

Entro tale contesto e, nonostante il Garante nazionale avesse rilasciato nel frattempo al Ministero dell'Interno un parere negativo per l'impiego di tecniche di riconoscimento facciale – per finalità di prevenzione e sicurezza – in contesti urbani [33], alcune città, tra le quali Torino e Venezia, valutavano l'inserimento di questa particolare tipologia di software per le telecamere installate negli spazi pubblici della città. Ed è questo il caso del progetto ARGO che, nel frattempo, veniva avviato dal Comune di Torino [34]. Con questa iniziativa, si è proposto, al fine di incrementare «la sicurezza urbana, la sicurezza integrata e la *governance* della mobilità» [35], di potenziare una rete di videosorveglianza diffusa, in aggiunta alle videocamere già installate precedentemente, aventi funzioni di *crossing detection* (rilevazione del superamento di una linea predefinita), *intrusion detection* (rilevazione di intrusioni in una certa area), *region entrance* (rilevazione dell'entrata di una persona/veicolo in un'area predefinita), *region exiting* (il contrario della precedente) e *motion detection* (rilevazione del movimento di una persona/veicolo) [36]. Le fasi del progetto sarebbero state essenzialmente due: in primo luogo, l'operazione avrebbe coinvolto l'area periferica [37] e successivamente quella centrale della città [38].

---

esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[32] Da qui in avanti anche Garante nazionale o Garante privacy.

[33] Cfr. il capitolo IV, § 2.

[34] Cfr. http://www.comune.torino.it/circ7/cm/pages/ServeBLOB.php/L/IT/IDPagina/6837. L. CARRER, *Black Box. Sicurezza e sorveglianza nelle nostre città*, Ledizioni, Milano, 2023, p. 137.

[35] Cfr. https://servizi.comune.torino.it/consiglio/prg/web/scheda_atto.php?c_argomento =I202100288 e CITTÀ DI TORINO, *AxTO – Azioni per le periferie torinesi*, reperibile su http://www.comune.torino.it/arredourbano/bm~doc/relazione-generale-axto.pdf.

[36] Cfr. L. CARRER, *La soluzione "innovativa" di Torino*, 28 gennaio 2021, reperibile su https://www.hermescenter.org/la-soluzione-innovativa-di-torino-argo/.

[37] Cfr. https://servizi.comune.torino.it/consiglio/prg/web/scheda_atto.php?c_argomento= I202100288. V. anche CITTÀ DI TORINO, *AxTO – Azioni per le periferie torinesi*, reperibile su http://www.comune.torino.it/arredourbano/bm~doc/relazione-generale-axto.pdf.

[38] Il progetto è stato reso definitivo a ottobre 2020. Cfr. L. CARRER, *La soluzione "innovativa" di Torino*, 28 gennaio 2021, cit.

Le videocamere, in questo caso, a differenza del progetto del Comune di Como, non sarebbero state in grado di riconoscere i volti delle persone, ma solo di categorizzare le medesime in base al genere e agli indumenti indossati, ovvero di individuare la presenza di oggetti (per esempio cappelli, zaini e borse), ossia di estrarre i cd. "metadati" [39]. Al contempo però la tecnologia sarebbe stata in grado di monitorare costantemente gli spostamenti delle persone, rivelandosi in tal modo ben più intrusiva di quella progettata nel territorio comasco [40].

Per questa ragione, il Garante nazionale, in seguito ad un'istruttoria preliminare sul progetto, ha deciso di sospendere i lavori. Il rischio maggiore, secondo l'Autorità, sarebbe quello di collezionare una serie di dati classificando gli individui in base a categorie standard e potenzialmente discriminatorie, tenendo conto soprattutto che, come si approfondirà meglio più avanti [41], diversi studi empirici dimostrano che anche gli algoritmi più avanzati possono commettere errori nella distinzione tra identità di genere e sesso biologico, oppure quando i destinatari coinvolti fanno parte di minoranze etniche [42].

Il progetto, per come originariamente formulato, è stato dunque temporaneamente sospeso. La controversia sulla raccolta dei metadati ha condotto, nel 2022, ad una rimodulazione delle condizioni dell'iniziativa, prevedendo che le telecamere non siano in grado di analizzare le immagini e di categorizzare i dati [43].

Un altro esempio paradigmatico è stato quello del Comune di Venezia. Il sistema, messo a punto nell'ambito del progetto "*Smart Control Room*" [44], è

---

[39] Ossia dati che precisano condizioni oggettive riferite alla genesi del dato.

[40] Cfr. E. D'ALBERGO-T. FASCIANI-G. GIOVANELLI, *La governance dell'Intelligenza Artificiale nelle politiche locali: trade-off e potere nel caso della videosorveglianza a Torino*, in *Riv. trim. Sc. amm.*, 4, 2023, p. 13.

[41] Cfr. il capitolo II, § 4.6.

[42] Cfr. M. MILLAR, *Facial recognition technology struggles to see past gender binary*, 30 ottobre 2019, reperibile su https://www.reuters.com/article/us-usa-lgbt-facial-recognition/facial-recognition-technology-struggles-to-see-past-gender-binary-idUSKBN1X92OD?edition-redirect=uk.

[43] Risposta all'interpellanza 2023-00105, Consiglio Comunale Città di Torino (2023).

[44] Cfr. E. MUREDDU, *Come Venezia è diventata il grande fratello d'Europa*, 27 ottobre 2021, reperibile su https://europa.today.it/attualita/venezia-grande-fratello.html e GREENS/EFA IN THE EUROPEAN PARLIAMENT, *Biometric Behavioural Mass Surveillance in EU Member States*, 2021, reperibile su http://extranet.greens-efa.eu/public/media/file/1/7297.

costituito da un *server* in grado di aggregare e controllare telecamere dotate di una tecnologia che permette di prevedere gli eventi metereologici, definendo percorsi alternativi per il transito nella città, indicare alla popolazione *in tempo reale*[45] i percorsi da evitare per il traffico, gestire la mobilità ottimizzandone i tempi, controllare l'occupazione dei parcheggi e monitorare costantemente l'afflusso dei visitatori.

Anche in questo caso, sono stati sollevati alcuni dubbi circa l'effettiva legittimità dell'impiego sistematico di siffatti strumenti da parte delle pubbliche amministrazioni[46], ma il progetto, non essendo basato sulla raccolta e conservazione dei dati biometrici, è stato portato avanti e risulta attuato. L'assenza di una banca dati centralizzata destinata alla memorizzazione dei dati biometrici ha ridotto le possibilità di configurazione di una sorveglianza indiscriminata. Nonostante ciò, i dubbi permangono, soprattutto in relazione alla possibilità che, anche in assenza di una raccolta strutturata dei dati biometrici, l'utilizzo della tecnologia implementata possa comunque dar luogo a forme di profilazione e identificazione massiva, incidendo in modo significativo sui diritti fondamentali degli individui[47].

Da ultimo, vale la pena richiamare brevemente anche il caso del Comune di Trento, sanzionato nel 2024 dal Garante privacy, per aver condotto due progetti di ricerca utilizzando telecamere, microfoni e reti neurali in violazione della normativa sulla protezione dei dati[48]. Oggetto di sperimentazione erano due sistemi di intelligenza artificiale, "*Marvel*"[49] e "*Protector*"[50], nell'ambito dei quali venivano raccolte informazioni in luoghi pubblici, attraverso microfoni e videocamere di sorveglianza, con il proposito di rilevare potenziali situazioni di pericolo per la sicurezza pubblica.

---

[45] Cfr. il capitolo II, § 4.

[46] Anche nel Comune di Udine, è stata annunciata la volontà di installare un nuovo sistema di videosorveglianza, con 67 nuove telecamere, in aggiunta alle 75 già presenti nella città e agli 11 sistemi di lettura delle targhe dei veicoli. La proposta era quella di implementare gli strumenti di video-analisi, come il riconoscimento di mezzi e individui in base ad una serie di criteri come, per esempio, l'età, il sesso, gli abiti, l'orario, attraverso l'impiego di software di analisi forense. Cfr. https://www.ilgiornalediudine.com/cronaca/green-pass-e-riconoscimento-facciale-udine-punta-a-un-sistema-di-sorveglianza-cinese/.

[47] Cfr. il capitolo III.

[48] Cfr. per un approfondimento A. FARANDA, *L'implementazione di sistemi di AI per la sorveglianza nei luoghi pubblici: il caso del Comune di Trento*, in *MediaLaws*, 16 aprile 2024.

[49] Cd. *Multimodal Extreme Scale Data Analytics for Smart Cities Environments*.

[50] Cd. *PROTECTing places of wORship*.

Più specificamente, con il primo si consentiva la raccolta e l'analisi di dati audiovisivi. Il progetto *Protector*, invece, rendeva possibile l'acquisizione di dati provenienti da telecamere di videosorveglianza e dati testuali derivanti da alcuni *social media* con lo scopo di migliorare la protezione dei luoghi di culto a livello urbano, attraverso l'analisi delle potenziali minacce terroristiche e la valutazione delle misure fornite dalle forze dell'ordine in tali contesti.

Rispetto ai due sistemi, il Garante ha ritenuto di sanzionare il Comune «per aver posto in essere trattamenti di dati personali in maniera non conforme al principio di liceità, correttezza e trasparenza, in violazione dell'art. 5, par. 1, lett. a) del Regolamento (UE) 2016/679; in assenza di base giuridica, in violazione degli artt. 6, 9 e 10 del Regolamento (...); omettendo di fornire agli interessati taluni degli elementi informativi richiesti dalla disciplina in materia di protezione dei dati, in violazione degli 13, par. 1, lett. c) ed e), e par. 2, lett. a), b) e d), e 14 del Regolamento; comunicando a terzi dati personali, anche relativi a reati e a categorie particolari (convinzioni religiose); omettendo di stipulare un accordo sulla protezione dei dati con la Fondazione (responsabile del trattamento), in violazione dell'art. 28 del Regolamento; omettendo di redigere una valutazione d'impatto sulla protezione dei dati conforme ai requisiti previsti dalla normativa in materia di protezione dei dati, in violazione dell'art. 35 del Regolamento» [51]. Inoltre, le tecniche di pseudonimizzazione messe in atto dal Comune non sono state ritenute idonee «ad assicurare l'effettiva anonimizzazione dei dati, atteso che gli interessati sono comunque potenzialmente identificabili tramite altre caratteristiche fisiche o elementi di contesto (come, ad esempio, la corporatura, l'abbigliamento, la posizione nella scena filmata, le caratteristiche fisiche particolari, ecc.) o informazioni provenienti da terzi (come, ad esempio, notizie di stampa relative a fatti di cronaca, informazioni fornite da persone presenti nella scena filmata, ecc.) o ancora informazioni desumibili, ad esempio, dalla localizzazione della telecamera (aree prospicenti determinati esercizi commerciali, studi medici o scuole) o, infine, informazioni relative al percorso effettuato da una determinata persona individuata nelle immagini video mediante le predette caratteristiche fisiche e gli elementi di contesto, stante la possibilità di seguire i suoi spostamenti fra le diverse telecamere installate».

L'Autorità, alla luce del funzionamento tecnico di entrambi i sistemi, ha stabilito che «il Comune, nell'ambito dei progetti "Marvel" e "Protector",

[51] Cfr. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/ 9977299.

ha trattato dati personali, anche relativi a reati e appartenenti a categorie particolari, contravvenendo alla ragionevole aspettativa di riservatezza degli interessati, in maniera non conforme al "principio di liceità, correttezza e trasparenza" e in assenza di base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6, 9 e 10 del Regolamento, nonché 2-*ter*, 2-*sexies* e 2-*octies* del Codice».

Il trattamento da parte del Comune dei dati personali, dei cittadini, giudicato non conforme alla normativa, ha portato ad una sanzione, sebbene il Garante abbia riconosciuto un comportamento «in buona fede, essendo [l'Amministrazione] incorsa in un errore in diritto, nella convinzione che i trattamenti in questione potessero essere sussunti nel quadro giuridico in materia di sicurezza urbana e che le misure volte all'anonimizzazione dei dati fossero sufficienti a evitare la possibilità di identificare gli interessati».

È interessante ricordare che, nel definire l'importo della sanzione inflitta [52], il Garante ha considerato tra le attenuanti anche il «numero limitato di ore di registrazione» (309 ore per il progetto Marvel e 18 ore per il progetto Protector, di cui solo 4 ore sono attualmente conservate) e la promozione di «forme di divulgazione pubblica dei progetti».

Anche nel caso del Comune di Trento, dunque, l'Autorità ha rimarcato che talune forme di sorveglianza negli spazi pubblici possono modificare il comportamento delle persone e condizionare l'esercizio delle libertà democratiche, e, per tale ragione, si è dichiarata aperta al dialogo, sia con il Comune di Trento, sia con ogni altra amministrazione pubblica, al fine di fornire supporto in vista di ogni eventuale futura iniziativa legata all'impiego dell'intelligenza artificiale per il trattamento dei dati biometrici, da realizzare in conformità con la normativa nazionale in vigore.

3. *La corsa alla regolamentazione*

Contestualmente al diffondersi delle suddette iniziative da parte dei Comuni, era stato presentato in Parlamento un disegno di legge volto, invece, a sospendere l'impiego delle tecnologie in questione [53]. Nel preambolo

[52] Il Garante ha irrogato una sanzione di 50.000 euro al Comune di Trento.

[53] Cfr. il d.d.l. AC 3009, "*Sospensione dell'installazione e dell'utilizzazione di impianti di*

dell'iniziativa normativa si evidenziava come un numero sempre maggiore di Comuni italiani, inclusi i principali capoluoghi, stesse pianificando la trasformazione dei propri sistemi di videosorveglianza in strumenti avanzati di riconoscimento facciale. Al contempo, si denunciava l'assenza di un quadro normativo uniforme che regolamentasse l'utilizzo dei dati biometrici da parte degli enti territoriali, in particolare per le attività di polizia giudiziaria svolte a livello locale. In tale contesto, la proposta legislativa mirava a introdurre una moratoria sull'impiego dei sistemi di riconoscimento facciale nei luoghi pubblici o aperti al pubblico, da mantenersi fino all'adozione di una disciplina normativa in grado di garantire il pieno rispetto dei diritti costituzionali dei cittadini, in conformità con le direttive delle autorità nazionali ed europee preposte alla protezione dei dati personali.

L'iniziativa normativa ha trovato concretizzazione nel d.l. n. 139/2021 (c.d. decreto "capienze"), successivamente convertito con modificazioni nella legge n. 205/2021 [54].

In particolare, l'art. 1 comma 9 ha stabilito la sospensione dell'installazione e dell'utilizzo di impianti di videosorveglianza dotati di sistemi di riconoscimento facciale, in luoghi pubblici o aperti al pubblico, sia da parte di autorità che di soggetti privati. Tuttavia, la norma ha specificato che la moratoria non si applica ai trattamenti effettuati dalle autorità competenti per finalità di prevenzione e repressione dei reati. In questi casi, il trattamento dei dati biometrici rimane subordinato all'acquisizione di un parere favorevole da parte del Garante per la protezione dei dati personali. A quest'ultima ulteriore previsione, fanno eccezione i casi in cui il sistema di riconoscimento facciale sia attivato direttamente dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali o investigative [55].

Un'analisi dettagliata delle disposizioni sopra menzionate e delle loro implicazioni giuridiche sarà sviluppata nei capitoli successivi [56]. In questa sede,

---

videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici in luoghi pubblici o aperti al pubblico", 12 aprile 2021, http://documenti.camera.it/leg18/pdl/pdf/leg.18.pdl.camera.3009.18PDL0137680.pdf.

[54] Cfr. il d.l. n. 139/2021 convertito con modificazioni in legge n. 205/2021 "*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*", le cui disposizioni sono state prorogate sino al 31 dicembre 2025 dal d.l. n. 51/2023, convertito con modificazioni dalla legge n. 87/2023.

[55] Cfr. l'art. 9, comma 12, d.l. n. 139/2021.

[56] Cfr. il capitolo IV, § 2.1.

è sufficiente evidenziare come il legislatore nazionale abbia riconosciuto la crescente pervasività e la progressiva diffusione della tecnologia di riconoscimento facciale, nonché la complessità del suo impiego nei diversi contesti applicativi. Tale consapevolezza si accompagna a un'esplicita attenzione ai rischi derivanti dall'utilizzo di questi strumenti, in particolare rispetto a specifici settori, nei quali il bilanciamento tra esigenze di sicurezza e tutela dei diritti fondamentali si rivela particolarmente critico[57]. L'adozione di una moratoria, seppur circoscritta e temporalmente delimitata, infatti, costituisce un chiaro indice della necessità di un intervento regolatorio più strutturato e meditato, volto a definire un quadro normativo capace di disciplinare in modo coerente e proporzionato l'impiego del riconoscimento facciale, evitando sia un utilizzo indiscriminato che un'irragionevole limitazione delle potenzialità offerte dalla tecnologia.

La stessa consapevolezza – nell'ultimo decennio – ha mosso, più ampiamente, numerose organizzazioni, governative e non governative, europee ed internazionali, ad adoperarsi per delineare le "coordinate" normative e paranormative in grado di orientare e disciplinare il comportamento degli operatori nel settore del riconoscimento facciale[58].

Già a partire dalla Risoluzione del 2019 su "*Una politica industriale europea globale in materia di robotica e intelligenza artificiale*", il Parlamento europeo aveva espresso una particolare preoccupazione per l'impiego di alcuni software di intelligenza artificiale[59], ivi compreso il riconoscimento facciale e vocale, in programmi di cd. "sorveglianza emotiva", ossia di monitoraggio degli stati d'animo degli individui (*sentiment analysis*), al fine di aumentare la produttività e conservare la stabilità sociale[60].

La Commissione europea, nel *White Paper* del 2020, aveva evidenziato alcune perplessità rispetto ai software di identificazione biometrica a distanza, e all'«impiego del riconoscimento facciale negli spazi pubblici», in quanto portatore di «specifici rischi per i diritti fondamentali»[61]. Già in una

---

[57] Cfr. il capitolo III.

[58] Cfr. il capitolo IV, § 3.

[59] Da ora in avanti anche semplicemente "IA". Come si approfondirà meglio nel capitolo II, § 4.3, il funzionamento della maggior parte delle più moderne tecnologie di riconoscimento facciale è basato sull'impiego delle tecniche di intelligenza artificiale.

[60] *Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale* (2018/2088(INI)), 12 febbraio 2019, p. 13.

[61] Cfr. *White Paper on Artificial Intelligence: a European approach to excellence and trust*, 19 febbraio 2020, p. 20 ss.

delle prime bozze preliminari del documento era stata prospettata la possibilità di proibire l'uso di queste tecnologie da parte di soggetti pubblici e privati per un periodo variabile dai tre ai cinque anni [62]. Successivamente, anche il Garante europeo per la protezione dei dati [63] e il Parlamento europeo [64] si sono allineati a questo approccio. Quest'ultimo organo, con la "*Risoluzione sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale*" [65], aveva chiesto espressamente una moratoria sulla diffusione dei sistemi di riconoscimento facciale per le attività di contrasto [66], «finché le norme tecniche non possano essere considerate pienamente conformi con i diritti fondamentali, i risultati ottenuti siano privi di distorsioni e non discriminatori, il quadro giuridico fornisca salvaguardie rigorose contro un utilizzo improprio, un attento controllo democratico e adeguata vigilanza, e vi sia la prova empirica della necessità e proporzionalità della diffusione di tali tecnologie» [67].

Nell'ambito del Consiglio d'Europa, l'attenzione si è maggiormente concentrata sulla definizione di un quadro normativo generale per l'intelligenza artificiale [68]. In tale contesto, però, le "*Linee guida per l'uso del riconoscimento*

---

[62] Cfr. J. DELCKER-B. SMITH MEYER, *EU considers temporary ban on facial recognition in public spaces*, in *Politico*, 16 gennaio 2020, https://www.politico.eu/article/eu-considers-temporary-ban-on-facial-recognition-in-public-spaces/.

[63] Cfr. *Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust*, 29 giugno 2020, p. 66, https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf.

[64] Cfr. *Risoluzione del Parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale (2020/2013(INI))*, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_IT.html.

[65] Cfr. *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)), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_IT.html.

[66] «(…) a meno che non siano usate strettamente ai fini dell'identificazione delle vittime di reati». Cfr. *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*, cit., § 27.

[67] Cfr. il § 27.

[68] *Algorithms and Human Rights*, 2018, https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5; CEPEJ – *European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment*, reperibile su https://www.coe.int/en/web/ cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-sys

facciale nel settore pubblico e privato" [69], hanno rappresentato un primo tentativo di regolamentazione specifica, fornendo principi basilari destinati a orientare gli Stati membri nell'adozione di una normativa nazionale. Le indicazioni non vincolanti contenute nel documento si rivolgono ai legislatori nazionali, invitandoli a predisporre una cornice giuridica in grado di disciplinare lo sviluppo e l'impiego di tali tecnologie, affinché il ricorso a questi strumenti non comprometta il rispetto della dignità umana, dei diritti fondamentali e, più nello specifico, del diritto alla protezione dei dati personali.

In ambito europeo, come approfondito in seguito, la svolta si è avuta però solo con il recente regolamento (UE) 2024/1689 sull'intelligenza artificiale [70], anche noto come "*AI Act*" – punto di arrivo di una serie di precedenti iniziative di *soft law*, elaborate in seno alle istituzioni dell'Unione europea per uno sviluppo e un utilizzo di *tools* algoritmici sicuri ed affidabili nel mercato unico europeo. L'impiego dei sistemi di riconoscimento biometrico *in tempo reale*, all'interno di spazi accessibili al pubblico e per finalità di *law enforcement*, è stato oggetto di particolare attenzione da parte del legislatore europeo, in quanto considerato altamente intrusivo rispetto ai diritti e alle libertà fondamentali degli individui. Alla luce di tali criticità, il quadro normativo europeo ha previsto un divieto generale di utilizzo di questi sistemi, fatte salve alcune eccezioni che, sin dalla pubblicazione della proposta normativa da parte della Commissione, hanno sollevato dubbi interpretativi e questioni applicative di non poco rilievo.

Parallelamente, anche per l'uso di sistemi di riconoscimento biometrico *a posteriori* – ovvero impiegati per l'identificazione di soggetti attraverso il confronto con database preesistenti – sono state introdotte, per la prima volta, disposizioni specifiche che delineano una base normativa preliminare, destinata a essere sviluppata e integrata dai singoli Stati membri attraverso discipline nazionali più dettagliate.

Non è però ancora questa la sede per approfondire in che termini esatti

---

tems-and-their-environment; più recentemente, *Convenzione quadro sull'Intelligenza Artificiale e i diritti umani, la democrazia e lo Stato di diritto*, 2024, https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f la quale però non si sofferma su queste tecnologie. Più ampiamente si veda il capitolo IV, § 3 ss.

[69] Cfr. *Guidelines on Facial Recognition*, 2021, T-PD(2020)03rev4.

[70] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, 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).

le istituzioni europee siano intervenute. Il legislatore, a livello tanto europeo quanto nazionale, ha ormai preso atto dell'urgenza di superare la fase del mero dibattito teorico sulla materia e di avviare un percorso normativo ponderato e meditato, finalizzato a costruire un quadro regolatorio in grado di bilanciare l'innovazione tecnologica e la tutela dei diritti fondamentali.

La riflessione che seguirà sarà volta a individuare gli ambiti in cui si rende necessario un intervento normativo strutturato, con l'obiettivo di colmare le attuali incertezze applicative e di garantire un sistema di tutele che risponda ai principi di coerenza e uniformità regolatoria. La sfida attuale non è più quella di interrogarsi sull'opportunità di regolamentare queste tecnologie, ma quella di individuare strumenti normativi adeguati a garantire un equilibrio tra sicurezza, efficienza operativa e salvaguardia delle libertà individuali.

Capitolo II
Inquadramento tecnico-scientifico e funzionamento operativo degli strumenti

SOMMARIO: 1. Il percorso di analisi. – 2. *βίος* e *μέτρον*: una ricostruzione semantica della categoria di riferimento. – 2.1. Il dato biometrico nel recente quadro normativo. – 3. Le proprietà dei tratti biometrici e le classificazioni dei sistemi di riconoscimento. – 4. Il funzionamento tecnico della tecnologia di riconoscimento facciale. – 4.1. Le peculiarità del Sistema Automatico di Riconoscimento delle Immagini (SARI): contesto di riferimento e dettagli operativi. – 4.2. La banca dati AFIS – SSA. – 4.3. Tecniche di intelligenza artificiale e riconoscimento facciale. – 4.4. Il calcolo del rapporto di verosimiglianza nella scienza forense. – 4.5. Le finalità di verifica, identificazione e categorizzazione biometrica. – 4.5.1. Il riconoscimento delle emozioni. – 4.6. Livello di accuratezza e tipologie di errore nella tecnologia di riconoscimento facciale. – 5. Il ruolo assunto dalle informazioni biometriche e le categorie di riferimento.

1. *Il percorso di analisi*

La panoramica introduttiva dà conto della crescente diffusione della tecnologia di riconoscimento facciale e lascia intendere il progressivo interesse del legislatore multilivello per le poliedriche applicazioni e le numerose implicazioni di tali strumenti. L'emergere di un dibattito sul piano normativo intorno agli impieghi di questa tecnologia testimonia, infatti, la consapevolezza istituzionale circa l'impatto trasversale del riconoscimento biometrico, sia in termini di opportunità applicative che di criticità normative, etiche e sociali.

Prima di indagare il tema su un piano più squisitamente procedurale, però, occorre chiarire cosa la scienza intenda con "tecnologia di riconoscimento facciale", mettendo in evidenza gli elementi costitutivi e le categorie tecniche di riferimento. Un'analisi dei fondamenti e dei limiti derivanti dall'impiego di siffatti strumenti di riconoscimento all'interno del procedimento penale non può che partire da una ricostruzione dei presupposti

tecnici, delle soglie di errore, degli scopi di utilizzo e delle principali finalità applicative sfruttate nell'ambito processuale penale.

Lo studio sarà allora in parte dedicato a indagare le interconnessioni tra il funzionamento dei software di riconoscimento facciale e la disciplina scientifica di riferimento – la biometria – con particolare attenzione al ruolo assunto dai processi automatizzati e dalle tecniche di intelligenza artificiale [1]. Tali ambiti, profondamente correlati dal punto di vista metodologico, hanno conosciuto un'evoluzione significativa negli ultimi anni, determinando un'accelerazione dello sviluppo delle tecnologie di *facial recognition*, ampliandone il potenziale applicativo, in particolare nel settore del *law enforcement* [2].

In questa prospettiva, l'analisi sarà volta alla ricostruzione del *ciclo del dato biometrico*, attraverso il quale si sviluppa il procedimento di riconoscimento facciale, soffermandosi in particolare sul funzionamento degli strumenti attualmente in uso alle forze di polizia.

L'assenza di familiarità con questi strumenti rischia di compromettere l'efficacia del dibattito giuridico, portando a soluzioni normative o interpretative che risultano astratte e poco aderenti alle effettive modalità operative delle tecnologie impiegate. Prendere atto di questo non è più una mera scelta metodologica, ma una condizione necessaria affinché il giurista possa svolgere un'analisi consapevole e fondata, capace di confrontarsi con la realtà tecnologica senza incorrere in schematismi obsoleti o in soluzioni normative disallineate rispetto all'evoluzione scientifica in atto.

2. βίος *e* μέτρον: *una ricostruzione semantica della categoria di riferimento*

I volti degli individui fanno parte della più ampia classe dei "dati biometrici", i cui meccanismi di funzionamento e le specifiche proprietà sono da ricondurre ai principi e ai fondamenti della disciplina scientifica di

[1] Cfr. *infra* il § 4.3.

[2] Cfr. G. BELLOMO, *Biometria e digitalizzazione della pubblica amministrazione*, in L. FERRARA-D. SORACE (a cura di), *A 150 anni dall'unificazione amministrativa italiana*, Firenze University Press, Firenze, 2017, p. 59 ss.

riferimento, la biometria. Questa (dalle parole greche *βίος* = vita e *μέτρον* = conteggio o misura) può definirsi come la «disciplina che studia le grandezze biofisiche – sia fisiologiche, sia comportamentali – allo scopo di identificarne i meccanismi di funzionamento, di misurarne il valore e di indurre un comportamento desiderato in specifici sistemi tecnologici» [3]. Essa consiste, dunque, in una sistematizzazione dei parametri biometrici, applicabile a ipotesi sperimentalmente controllabili, attraverso il ricorso ad alcune tecniche specifiche [4].

Prima di trovare ampia diffusione nel settore della sicurezza e dell'informatica [5], la disciplina biometrica è stata principalmente sfruttata per l'analisi di metodi matematici e statistici applicati alla biologia, alle scienze agrarie e forestali, alla medicina, alla genetica e alle scienze ambientali [6]. Tra le finalità principali di tale settore scientifico rientrano lo studio della correlazione genetica tra le specie e le popolazioni, i dosaggi farmacologici, le diagnosi mediche e, infine, l'identificazione degli individui [7]. Invero, da sempre gli esseri umani si servono delle caratteristiche del proprio corpo (come il volto o la voce) per interagire con altri individui e con il mondo circostante [8]. Con

---

[3] Cfr. "Biometria" o "*Biometry*", Enciclopedie *online* – Istituto dell'Enciclopedia italiana Treccani, http://www.treccani.it/enciclopedia/biometria/.

[4] Cfr. più ampiamente G. PREITE, *Politica e biometria. Nuove prospettive filosofiche delle scienze sociali*, Tangram Edizioni Scientifiche, Trento, 2016, p. 21.

[5] Cfr. E. MORDINI, *Il Volto e il Nome. Implicazioni Etiche, Sociali e Antropologiche delle Tecniche di Identificazione Biometriche*, in *MEDIC*, 14, 2006, p. 31, parla a tal proposito di «moderna biometria».

[6] Sul punto si veda il sistema di Classificazione Decimale Dewey (CDD) in cui la "biometria" è accorpata alla "biostatistica" (CDD: 574.015195), classificata nella materia "scienze naturali e matematica" (CDD: 500), alla classe "scienze della vita" (CDD: 574), per la sezione "filosofia e teoria" (CDD:574.01), in L. CROCETTI-D. DANESI (eds.), *Classificazione decimale*, Dewey, Ed. n. 20, Vol. II, Roma, AIB, 1993. Si veda anche G. MONTECCHI-F. VENUDA, *Manuale di biblioteconomia*, Editrice Bibliografica, Milano, 1999, p. 124 e 243; K. MATHER, *Elementi di biometria*, Boringheri, Torino, 1972, p. 3 ss.

[7] Il campo di applicazione risulta estremamente vasto riguardando tutto ciò che è legato ad una qualche misurazione della vita: dalla biometria vegetale che consente per esempio di stabilire l'età di una specie botanica, alla biometria animale che classifica e analizza le caratteristiche principali degli animali, ovvero una biometria medica che costituisce la base conoscitiva dei principali esami clinici (per es. una TAC o una RMN).

[8] Cfr. S. AMATO-F. CRISTOFARI-S. RACITI, *Biometria. I codici a barre del corpo*, Giappichelli, Torino, 2013, p. 4 ss.; B. LAVANYA-H. HANNAH INBARANI, *A Survey of Biometric Techniques*, in *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(7), 2015. «L'identificazione degli esseri umani è un'esigenza cognitivamente e

l'evoluzione delle strutture sociali e l'aumento della complessità dei rapporti interpersonali, è emersa l'esigenza di riconoscere gli individui, attribuendo al corpo umano il ruolo di mezzo immediato e naturale di identificazione [9].

L'avanzamento tecnologico ha contribuito in modo significativo a trasformare tale funzione in un processo sempre più strutturato e automatizzato, in particolare nel settore della sicurezza. L'impiego del corpo umano a fini identificativi ha progressivamente assunto una dimensione scientifica e tecnologica, dando luogo allo sviluppo di sistemi biometrici avanzati, capaci di estrarre e analizzare caratteristiche uniche e distintive per verificare o confermare l'identità di un soggetto [10]. Con riferimento a questo particolare ambito di applicazione, la società internazionale *International Biometric Group* (da qui in avanti "IBG"), riconosciuta come punto di riferimento in materia, ha precisato che con il termine "*biometrics*" si intende l'«uso automatizzato di caratteristiche fisiologiche o comportamentali per determinare o verificare l'identità» [11]. Tale definizione evidenzia il passaggio da un approccio empirico e soggettivo, basato su misurazioni analogiche, a un modello tecnologico e standardizzato, in cui i metodi di

---

psicologicamente fondamentale che si è manifestata senza eccezioni in ogni società», COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, 2010, p. 4.

[9] Per una ricostruzione sul tema cfr. S. AMATO-F. CRISTOFARI-S. RACITI, *Biometria: I codici a barre del corpo*, Giappichelli, Torino, 2013 e G. PREITE, *Il riconoscimento biometrico – Sicurezza versus privacy*, Uni Service, Trento, 2007.

[10] Per un'analisi in prospettiva storica cfr. M. PULICE, *Sistemi di rilevazione di dati biometrici e privacy*, in *Lav. giur.*, 10, 2009, 994, p. 2; A. GIULIANO, *Dieci e tutte diverse. Studio sui dermatoglifi umani*, Tirrenia Stampatori, Torino, 2004, p. 1 ss.; G. IOVANE, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza*, Aracne, Roma, 2008, p. 174 ss.; E. MORDINI-C. PETRINI, *Ethical and social implications of biometric identification technology*, in *Ann. Ist. Super. Sanità*, 43(1), 2007, p. 5-11, e, con riferimento all'impatto del progresso scientifico sulla disciplina biometrica, v. A.K. JAIN-S. PANKANTI-S. PRABHAKAR-L. HONG-A. ROSS-J.L. WAYMAN, *Biometrics: A Grand Challenge*, in *Proceedings of International Conference on Pattern Recognition*, Cambridge, UK, 2004.

[11] L'*International Biometric Group* è una società professionale accademica internazionale che offre servizi nel settore della biometria sia nell'ambito pubblico che nell'ambito privato. Il termine "biometria" si riferisce a «*the automated use of physiological or behavioural characteristics to determine or verify identity*», INTERNATIONAL BIOMETRIC GROUP, *How is "biometrics" defined?*, in http://www.biometricgroup.com/public/reports/biometric/definition.htlm. L'OECD (ORGANIZZAZIONE PER LA COOPERAZIONE E PER LO SVILUPPO ECONOMICO) – nel 2004 – ha fatto propria tale definizione nel documento WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-based technologies*, p. 10 e 11.

riconoscimento giocano un ruolo determinante nel processo di identificazione e autenticazione.

L'impiego dell'aggettivo "automatizzato" evidenzia la necessità che il riconoscimento sia eseguito senza un intervento umano continuativo. Questo elemento distintivo consente di differenziare le tecnologie biometriche basate su procedure analogiche da quelle che si avvalgono di sistemi computazionali avanzati, capaci di elaborare e confrontare i dati biometrici in maniera autonoma e standardizzata. Tale caratteristica assume una rilevanza particolare nell'ambito delle moderne applicazioni di riconoscimento facciale, che si fondano su modelli di intelligenza artificiale per acquisire, analizzare e validare le informazioni biometriche [12].

Nel contesto attuale, caratterizzato da una rapida evoluzione delle tecnologie di identificazione personale, risulta legittimo interrogarsi sulla sopravvivenza di tecniche biometriche esclusivamente analogiche. Sebbene in alcune circostanze residuali – ad esempio in ambito forense tradizionale – si possa ancora rilevare l'impiego di misurazioni biometriche a carattere manuale, appare ormai evidente che tali modalità rappresentano l'eccezione piuttosto che la regola. Ciò che connota in modo decisivo la transizione in atto è la tendenziale e sistematica automazione dei processi di acquisizione, elaborazione e comparazione del dato biometrico, una trasformazione strutturale resa possibile dall'integrazione pervasiva di architetture di calcolo avanzate.

L'IBG sottolinea poi che un sistema biometrico digitale non si esaurisce nella mera implementazione di un modello di riconoscimento, ma si configura come un'architettura tecnologica complessa, composta da una pluralità di componenti infrastrutturali imprescindibili per il suo corretto funzionamento e per l'affidabilità dei risultati prodotti. In particolare, un sistema biometrico è composto da elementi *hardware* (sensori e dispositivi di acquisizione), *software* (algoritmi di elaborazione e confronto), *firmware* (moduli integrati per la gestione delle operazioni) e componenti di rete, necessari per garantire la trasmissione, l'archiviazione e la gestione sicura dei dati. Questa precisazione è tesa a evidenziare la natura multidimensionale della biometria, la quale non può essere ridotta a una mera operazione di identificazione individuale, ma deve essere considerata come un'infrastruttura tecnologica complessa, il cui funzionamento dipende dall'interazione tra diverse discipline.

Parallelamente, l'Agenzia governativa statunitense *National Science and Technology Council* (da qui in avanti "NSTC") e il sottocomitato sulla

[12] Cfr. *infra* il § 4.3.

biometria hanno precisato che per "*biometrics*" si debba intendere la «caratteristica biologica (anatomica e fisiologica) e/o comportamentale che può essere usata per riconoscimenti automatizzati»[13]. A differenza della definizione proposta dall'IBG, questa formulazione non implica necessariamente che il sistema biometrico sia in grado di determinare univocamente o verificare con certezza l'identità dell'individuo. Piuttosto, essa si limita a considerare le caratteristiche biometriche come elementi suscettibili di essere utilizzati nei processi di riconoscimento, senza presupporre un'esatta corrispondenza identitaria. Infatti, mentre l'IBG enfatizza la finalità identificativa o verificativa del sistema biometrico, attribuendo centralità al funzionamento automatizzato, la definizione del NSTC adotta un approccio più ampio, riconoscendo la biometria come la disciplina che studia l'insieme delle caratteristiche fisiche o comportamentali che possono essere utilizzate nei processi di analisi senza necessariamente implicare l'identificazione univoca del soggetto. La distinzione concettuale non è priva di conseguenze, poiché incide sulle modalità di regolamentazione dei sistemi biometrici e sulla definizione dei limiti normativi entro i quali tali tecnologie possono essere impiegate.

Al fine di pervenire a un'interpretazione condivisa, un contributo essenziale è stato fornito dal Consiglio d'Europa e dall'Unione europea, nei cui contesti numerosi enti e istituzioni hanno progressivamente rivolto la loro attenzione alle implicazioni derivanti dalla diffusione su larga scala di sistemi biometrici integrati con tecniche di intelligenza artificiale[14]. Il crescente impiego di queste tecnologie ha infatti sollevato interrogativi di natura giuridica, etica e tecnologica, rendendo necessaria una riflessione approfondita sulla loro regolamentazione e sui limiti della loro applicabilità.

Le prime fonti non sono riconducibili al diritto positivo, trattandosi principalmente di rapporti, raccomandazioni e linee guida. Nonostante l'assenza di valore cogente, tali documenti hanno assunto un'importanza significativa sotto diversi profili. Da un lato, il prestigio degli enti di ricerca coinvolti ha conferito autorevolezza alle analisi effettuate; dall'altro, il carattere interdisciplinare delle riflessioni contenute in questi documenti ha consentito di

---

[13] Il NATIONAL SCIENCE TECHNOLOGY COUNCIL è un organo consultivo interno al governo federale degli Stati Uniti d'America. È stato istituito il 23 novembre 1993 dal Presidente Bill Clinton con la specifica funzione di coordinamento della politica in ambito scientifico e tecnologico. Cfr. DEP. OF DEFENCE USA, *Report of the Defense Science Board Task Force on Defence Biometrics*, p. 8, D.C. 20301-2140, 2007: «*a measurable biological (anatomical and physiological) and/or behavioural characteristic that can be used for automated recognitions*».

[14] Cfr. il capitolo II, § 4.3.

delineare un quadro più ampio degli impatti della biometria, non limitandosi alla sua dimensione strettamente tecnologica, ma estendendo l'indagine alle ripercussioni di ordine giuridico e sociale. Inoltre, tali studi hanno rappresentato un punto di riferimento fondamentale per i successivi interventi normativi, fornendo la base concettuale per lo sviluppo di regolamentazioni più strutturate. A tal proposito, si ricorda il "*Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*", del 2005, relativo all'applicazione ai dati biometrici della Convenzione 108 del 1981 del Consiglio d'Europa, sulla protezione degli individui riguardo al trattamento automatizzato di dati personali [15] che – più genericamente – considera la biometria come «*a traditional method of identification of individuals*» [16]. Questa prospettiva mette in luce come l'impiego delle caratteristiche biometriche ai fini identificativi non rappresenti un fenomeno recente, bensì costituisca l'esito di un'evoluzione tecnologica di pratiche di riconoscimento e autenticazione già consolidate nel tempo. L'innovazione introdotta dai sistemi automatizzati non risiede, dunque, nella logica sottostante all'identificazione dell'individuo, che affonda le proprie radici in pratiche antropometriche tradizionali, bensì nella capacità delle moderne tecnologie di elaborare grandi volumi di dati biometrici in tempi estremamente ridotti, garantendo un'elevata capacità di adattamento in diversi contesti applicativi e implementazione su ampia scala.

Quasi contestualmente il *Joint Research Center*, servizio scientifico della Commissione europea, ha condotto uno studio sulle implicazioni etiche e giuridiche derivanti dal trattamento dei dati biometrici, definendo questi ultimi come «*any human physical or biological feature that can be measured and used for the purpose of automated or semi-automated identification*» [17].

---

[15] Cfr. *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, in https://rm.coe.int/16806840ba, 2005. La Convenzione 108 del 1981 (*Convention for the protection of individuals with regard to automatic processing of personal data*), anche a seguito dell'introduzione del protocollo di aggiornamento nel 2018 (Convenzione 108+), ha dato attuazione all'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950, definendo i principi per la tutela della vita privata delle persone.

[16] Cfr. *Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, cit., p. 2.

[17] EUROPEAN COMMISSION, *Biometrics at the Frontiers: assessing the impact on society. For the European Parliament Committee on Citizen's Freedom and Rights, Justice and Home Affaire (LIBE)*, 2005.

Rispetto all'approccio adottato dal Consiglio d'Europa, tale impostazione si distingue per una maggiore enfasi sulla dimensione tecnologica del dato biometrico, ampliando la prospettiva oltre le sue tradizionali applicazioni identificative. In questa concezione, il dato biometrico non viene considerato esclusivamente come uno strumento di riconoscimento individuale, ma anche come un elemento informativo polifunzionale, suscettibile di impieghi che non necessariamente implicano un accertamento identitario diretto. L'interpretazione evidenzia il carattere dinamico e adattabile dei dati biometrici, che possono essere utilizzati anche per finalità predittive, analitiche o di categorizzazione, oltre che per il riconoscimento dell'identità.

Nel contesto italiano, una prima definizione della disciplina è stata fornita dal Comitato nazionale per la bioetica, che ha inteso la disciplina come una nuova tecnica «di identificazione o "misurazione" dell'essere umano attraverso la rilevazione di determinate caratteristiche fisiche e comportamentali che vengono tradotte in sequenze matematiche e conservate in banche dati elettroniche» [18]. La nozione mette in luce due elementi distintivi della biometria, che ne definiscono la natura e il funzionamento all'interno dei moderni sistemi di identificazione automatizzata. Da un lato, essa si fonda sulla misurazione e sulla quantificazione di caratteristiche fisiologiche o comportamentali, individuate sulla base di parametri distintivi per ciascun individuo. Dall'altro, affinché tali informazioni possano essere utilizzate nei processi di riconoscimento automatizzato, è imprescindibile che esse siano digitalizzate e archiviate all'interno di sistemi informatici. La conversione delle caratteristiche biometriche in formati digitali strutturati consente non solo la loro memorizzazione e gestione, ma anche la successiva elaborazione

[18] COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, cit., p. 3. Precedentemente, un riferimento alla disciplina biometrica si rinviene nell'art. 1, lett. *g*), d.P.R. n. 513/1997 ("*Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici*") che, nel qualificare giuridicamente il documento informatico e la firma digitale, ha definito "chiave biometrica" la «sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità digitale basati su specifiche caratteristiche fisiche dell'utente». Successivamente, l'art. 8, comma 3, d.P.R. n. 445 del 2000 ha ridefinito le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico anche con riferimento all'eventuale uso di chiavi biometriche. Con il d.lgs. 30.6.2003 n. 196 il legislatore ha riconosciuto la rilevanza dei dati biometrici come una particolare tipologia di informazioni personali per la quale è previsto l'obbligo della notifica all'Autorità Garante (art. 37, comma 1, lett. *a*) per la natura del trattamento ritenuto più delicato rispetto ad altri, senza, peraltro, mai fornire una puntuale definizione.

mediante algoritmi di intelligenza artificiale e *machine learning* [19], i quali eseguono il confronto tra i dati acquisiti e quelli già presenti nei database. Questa duplice dimensione della biometria – da un lato biologica e comportamentale, dall'altro tecnologica e computazionale – ne determina la specificità rispetto ad altre metodologie di identificazione.

La pluralità di definizioni adottate da differenti organismi nazionali e sovranazionali testimonia l'assenza di un linguaggio giuridico e tecnico uniformemente codificato, determinando divergenze nell'applicazione della normativa, influenzando la regolamentazione del trattamento dei dati biometrici e delle tecnologie di identificazione automatizzata. Questa frammentazione concettuale si traduce in una disomogeneità nell'elaborazione delle politiche pubbliche, rendendo più complessa l'armonizzazione del quadro normativo a livello internazionale e la definizione di standard operativi chiari. Come visto, alcune definizioni enfatizzano l'origine biologica o comportamentale del dato biometrico, evidenziandone la natura di caratteristica intrinseca dell'individuo; altre, invece, pongono l'accento sulla sua finalità, ovvero la possibilità di impiegarlo per la verifica e l'identificazione automatizzata di una persona. Se, da un lato, tale pluralità di prospettive è comprensibile – in considerazione della trasversalità della disciplina e delle sue numerose applicazioni nei settori della sicurezza, della sanità, dei servizi digitali e della sorveglianza – dall'altro urge l'inserimento di una definizione univoca e universalmente accettata di dato e sistema di riconoscimento biometrico [20].

L'*International Standard Organization* (ISO/IEC 2382-37) ha, perciò, operato un primo tentativo di sistematizzazione di tutte le definizioni fornite – nei diversi ambiti – al fine di armonizzare da un punto di vista tassonomico la materia [21]. In particolare, per "dato biometrico" s'intende «*[the] biological or behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition*». È definito "*biometric recognition*", invece, «[the] *recognition of*

[19] Cfr. più ampiamente il capitolo II, § 4.3.

[20] «La difficoltà nell'individuazione di una convenzione definitoria è dovuta sia al fatto che manca nel panorama giuridico attuale una qualificazione normativa condivisa di tali categorie di dati, sia al fatto che il progresso della ricerca scientifica e l'evoluzione della tecnologia ampliano continuamente le possibilità di acquisizione e di elaborazione di questi dati vanificando ogni tentativo di fornire un'immagine statica della categoria». A. IANNUZZI-F. FILOSA, *Il trattamento dei dati genetici e biometrici*, in *Dirittifondamentali.it*, 2, 2019.

[21] Cfr. nella versione aggiornata, ISO/IEC 2382-37:2022, https://www.iso.org/standard/73515.html.

individuals based on their biological and behavioural characteristics, encompassing biometric verification and biometric identification». Permane il riferimento all'aggettivo "*automated*" nella definizione di «*biometrics*»[22], a sottolineare la centralità assunta dai processi automatizzati nell'acquisizione, elaborazione e utilizzo delle informazioni biometriche. Al contempo, la categoria di "dato biometrico" sembra comprendere sia il dato grezzo, inteso come l'insieme delle caratteristiche fisiche, fisiologiche o comportamentali dell'individuo, sia le sue rappresentazioni digitalizzate e i modelli elettronici derivati, funzionali all'identificazione, all'autenticazione o alla verifica automatizzata dell'identità. Viene posta in luce la duplice dimensione del dato biometrico: da un lato, esso si configura come un'informazione biologica originaria, direttamente riconducibile all'identità fisica del soggetto; dall'altro, assume una forma computazionale, traducendosi in codificazioni numeriche e algoritmiche che consentono il confronto automatizzato tra i profili biometrici registrati nei database e i dati acquisiti in tempo reale.

A livello europeo, una delle prime definizioni normative di "dato biometrico" è stata introdotta nel Parere 3/2012 del Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali (WP29)[23]. In tale documento, i dati biometrici vengono descritti come informazioni derivanti da proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili, nella misura in cui tali attributi risultano specifici di un determinato individuo e suscettibili di misurazione. Tuttavia, il WP29 evidenzia che i metodi tecnici utilizzati per la rilevazione

---

[22] Definita come «*automated recognition of individuals based on their behavioural and biological characteristics*». Cfr. ISO/IEC 2382-37:2022 e E. MICHELI TZANAKOU-K.N. PLATANIOTIS, *Biometrics: Terms and Definitions*, in H.C.A. VAN TILBORG-S. JAJODIA (a cura di), *Encyclopedia of Cryptography and Security*, Springer, Boston, 2011.

[23] Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali (Working Party 29) introdotto dall'articolo 29 della Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Cfr. C.A. JASSERAND, *Avoiding terminological confusion between the notions of 'biometrics' and 'biometric data': an investigation into the meanings of the terms from a European data protection and a scientific perspective*, in *International Data Privacy Law*, 6(1), 2016, p. 64, ove l'Autrice afferma che: «(…) *although the current version of the Standard is the first one published and might be subject to revision, it has already been quoted as a document of reference by national data protection authorities*», riferendosi proprio all'Autorità italiana e alle *Guidelines on Biometric Recognition and Graphometric Signature, Annex A to the Garante's Order of 12 November 2014.*

e l'analisi di tali caratteristiche operano su una base probabilistica, implicando che il risultato del processo biometrico non possa essere considerato univoco e assoluto. Questa impostazione concettuale si distingue per la sua flessibilità, riconoscendo la natura probabilistica delle tecnologie biometriche e la loro dipendenza da variabili contestuali e metodologiche, come la qualità dei dati raccolti, le condizioni ambientali e i margini di errore algoritmico. L'integrazione degli aspetti comportamentali nella definizione di dato biometrico contribuisce ad ampliare significativamente l'ambito di applicazione della categoria, estendendone la portata oltre i tradizionali tratti fisiologici statici – quali, ad esempio, le impronte digitali o la morfologia facciale – per includere anche caratteristiche dinamiche e ripetibili. Queste ultime, tra cui si annoverano i modelli vocali, la firma grafometrica e i *pattern* di digitazione, presentano una componente temporale e comportamentale che riflette non solo la struttura fisica dell'individuo, ma anche modalità di esecuzione riconducibili alla sua identità psico-motoria.

La stessa accezione è stata ripresa a sua volta dall'Autorità Garante per la protezione dei dati personali nelle "*Linee guida in materia di riconoscimento biometrico e firma grafometrica*" [24], ove la "caratteristica biometrica" è stata intesa come la qualità «biologica o comportamentale di un individuo da cui possono essere estratti in modo ripetibile dei tratti biometrici (*biometric features*) distintivi e idonei al riconoscimento biometrico» [25].

Quasi contestualmente, il Consiglio d'Europa nel documento "*Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*", nel definire il "dato biometrico", adotta un'impostazione terminologica maggiormente flessibile rispetto alle precedenti formulazioni normative in materia. In particolare, nel testo si afferma che «*biometric data (or biometrics) are measurable, physiological or behavioural characteristics that can be used to determine or verify identity. Biometrics is also defined as 'the automated use of physiological or behavioural characteristics to determine or verify individuals'*» [26]. Quindi, da un lato, i dati vengono intesi in senso generale, come le caratteristiche fisiologiche o comportamentali misurabili per finalità di identificazione o verifica. Dall'altro, il

[24] Cfr. *Linee guida in materia di riconoscimento biometrico e firma grafometrica*, allegato A al Provvedimento del Garante del 12 novembre 2014, reperibile su www.gpdp.it.

[25] Cfr. *Linee guida*, cit., p. 4.

[26] *Progress report on the application of the principles of convention 108 to the collection and processing of biometric data*, 2013, in https://rm.coe.int/progress-report-on-the-application-of-the-principles-of-convention-108/1680744d81.

documento riconduce il concetto di biometria alla sua dimensione computazionale, ovvero all'uso automatizzato dei dati per determinare o verificare l'identità di un individuo. Questa nozione, rispetto a quelle contenute in standard internazionali, quali la ISO/IEC 2382-37:2022, sembra non stabilire la necessità che il processo biometrico avvenga in via automatizzata. Ne consegue che, almeno sotto il profilo concettuale, potrebbe rientrare nella nozione di biometria anche un accertamento svolto in forma ibrida, con l'ausilio di strumenti tecnologici non integralmente automatizzati o mediante l'intervento umano nella fase di confronto o valutazione del dato.

2.1. *Il dato biometrico nel recente quadro normativo*

Con l'entrata in vigore del regolamento (UE) 2016/679 relativo alla protezione del trattamento dei dati personali (cd. GDPR)[27], è stata introdotta

[27] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (da qui in avanti anche "GDPR"). Il d.lgs. n. 101/2018, contenente le disposizioni per l'adeguamento della normativa nazionale ai principi del regolamento (UE) 2016/679, ha avuto la funzione di armonizzare le norme enunciate dal legislatore nazionale nel codice in materia di protezione dei dati personali (d.lgs. n. 196/2003) con quelle introdotte dal regolamento. Il regolamento ha abrogato le precedenti disposizioni contenute nella direttiva 95/46/CE (direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati – G.U. legge 23 novembre 1995, n. 281). Quest'ultima, conosciuta anche come "direttiva madre", non riconosceva la specificità dei dati biometrici e li faceva, perciò, rientrare nella generale categoria dei dati personali, che ricomprendeva «*qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identicazione o ad uno o più elementi o specifiche caratteristiche della sua identità fisica, fisiologica, psichica, economica, culturale o sociale*». A norma dell'art. 29 della direttiva 95/45/CE, era stato istituito il "Gruppo per la tutela dei dati personali" ossia un organo consultivo indipendente dell'Unione europea avente competenze in materia di tutela dei dati e della vita privata. Si deve a tale ente il merito di aver elaborato un documento di riferimento nel settore, il *Documento di lavoro sulla biometria*, nel quale sono stati specificati alcuni principi basilari aventi ad oggetto la natura dei dati biometrici e le modalità di trattamento (GRUPPO PER LA TUTELA DEI DATI PERSONALI – ARTICOLO 29, *Documento di lavoro sulla biometria*, 2003, in https://www.garanteprivacy.it/documents/10160/10704/443868.pdf/f6caf8cd-dcd3-426f-b64d-388a9863391a?version=1.0. Tale documento ha specificato che, con "sistemi biometrici", si vuole indicare le

una definizione normativa di dato biometrico, che sembra recepire gran parte delle caratteristiche distintive di questa categoria di informazioni, così come delineate nella letteratura scientifica e nei precedenti inquadramenti normativi. Tuttavia, nonostante il tentativo di sistematizzazione operato dal legislatore europeo, la definizione fornita dal GDPR non risulta esente da ambiguità interpretative, lasciando aperte alcune questioni circa la sua applicazione pratica e il perimetro esatto di tutela giuridica garantita.

L'art. 4(14) ha definito, infatti, "biometrici" «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»[28]. L'enunciazione suggerisce che, per essere considerati "biometrici", i dati personali devono soddisfare una serie di criteri[29]. Innanzitutto devono costituire "dati relativi a una persona fisica identificata o identificabile". L'interpretazione di questo requisito risulta piuttosto intuitiva e non solleva particolari problematiche ermeneutiche.

Il secondo criterio appare, invece, molto più controverso poiché il regolamento non chiarisce esplicitamente come debba essere interpretata l'espressione "trattamento tecnico specifico". In tal senso, il considerando 51

---

applicazioni di tecnologie biometriche che permettono l'identificazione e/o l'autenticazione/verifica automatica di un individuo. Il d.lgs. n. 196/2003, recante "Codice in materia di protezione dei dati personali" (d'ora in avanti, anche codice *privacy*), recependo le indicazioni dettate dalla direttiva, all'interno di un *corpus* normativo ora abrogato, aveva costruito una efficace cornice normativa per il trattamento dei dati genetici e biometrici, innanzitutto considerando l'informativa e il consenso. Il trattamento dei dati genetici e dei campioni biologici poteva avvenire solo previo consenso informato dell'interessato. Per un'efficace ricostruzione sul punto, cfr. A. IANNUZZI-F. FILOSA, *Il trattamento dei dati genetici e biometrici*, in *Diritti fondamentali.it*, 2, 2019; P. DE HERT, *Biometrics: legal issues and implications*, in *Background paper for the Institute of Prospective Technological Studies*, DG JRC – Sevilla, European Commission, January 2005 e F. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza artificiale*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018, p. 5 ss.

[28] L'accezione è stata fatta propria anche dalla direttiva 2016/680/UE del Parlamento europeo e del Consiglio del 27 aprile 2016, 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 dal d.lgs. n. 101/2018. Anche il regolamento (UE) 2018/1725, art. 3 (18), ha abbracciato la medesima definizione di "dato biometrico".

[29] Cfr. C. JASSERAND, *Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data*, in *European Data Protection Law Review* 2, n. 3, 2016, p. 297-311.

afferma che «il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica». Si osserva non solo un mutamento da "trattamento tecnico specifico" a "dispositivo tecnico specifico", ma cambia anche la finalità: da quella di "consentire" o "confermare" l'"identificazione univoca", all'"identificazione" o "autenticazione" di una persona fisica. Il tema è al centro di un ampio dibattito scientifico [30]. L'interpretazione prevalente della nozione di *specific technical processing* fa riferimento al procedimento mediante il quale un campione biometrico grezzo viene convertito in una rappresentazione digitalizzata, denominata *biometric sample*, ovvero trasformato nel relativo *template* biometrico [31], ossia il modello elettronico delle caratteristiche fondamentali di un dato tratto biometrico [32]. Quindi, solo attraverso un'ulteriore attività tecnica – consistente nell'analisi e nell'estrazione dei tratti biometrici significativi – si renderebbe possibile «l'identificazione univoca o l'autenticazione di una persona fisica», conformemente ai requisiti definiti dalla normativa in materia di protezione dei dati personali. Un'interpretazione estensiva della nozione di *specific technical processing* appare più giuridicamente e logicamente fondata, in quanto non è possibile limitare tale definizione esclusivamente alla fase di conversione del dato biometrico grezzo in un *template* digitale. Al contrario, la categoria deve ricomprendere tutte le operazioni che comportano un trattamento tecnico specifico dei dati biometrici, indipendentemente dalla natura del supporto utilizzato, purché finalizzate alla raccolta, registrazione, organizzazione, conservazione, elaborazione, estrazione e comparazione di tali dati. Questa prospettiva si giustifica in ragione del fatto che la conservazione e

[30] Cfr. E.J. KINDT, *Having yes, using no? About the new legal regime for biometric data*, in *Computer Law and Security Review*, 34, 2018.

[31] Le *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video* pubblicate dall'*European Data Protection Board* il 29 gennaio 2020 parlano più generalmente di "misurazioni" (il § 74 specifica che «per poter configurare un trattamento di dati biometrici, secondo la definizione del GDPR, il trattamento di dati grezzi, come ad esempio le caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, deve comprendere una misurazione di tali caratteristiche. Poiché i dati biometrici sono il risultato di dette misurazioni, il GDPR afferma nel suo articolo 4, paragrafo 14, che sono dati "[…] 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 […]"»).

[32] Cfr. § 4.

l'archiviazione di un dato biometrico, pur non essendo finalizzate direttamente all'identificazione o all'autenticazione immediata di un individuo, costituiscono comunque precondizioni indispensabili per il perseguimento di tali obiettivi. Infatti, l'efficacia di qualsiasi sistema di riconoscimento biometrico dipende non solo dalla qualità dei processi automatizzati di comparazione, ma anche dalla gestione sicura e strutturata dei dati biometrici raccolti, affinché essi possano essere utilizzati successivamente per l'identificazione o la verifica dell'identità [33].

Il terzo criterio di classificazione si riferisce alle qualità intrinseche degli individui, ovvero a quelle caratteristiche che risultano connaturate alla persona e non sono soggette a variazioni accidentali o contingenti. Tali qualità possono essere di natura fisica, fisiologica o comportamentale, e costituiscono il fondamento dell'identificazione biometrica in quanto elementi distintivi e relativamente stabili nel tempo. Queste caratteristiche si differenziano nettamente dalle qualità accidentali, le quali, pur essendo informazioni personali riconducibili a un determinato soggetto, non rappresentano attributi univoci e permanenti. Ne sono un esempio l'indirizzo di residenza, la posizione lavorativa in un dato momento storico, i dati relativi all'occupazione o altre informazioni suscettibili di modifiche nel corso della vita dell'individuo. Mentre i dati biometrici, come l'impronta digitale o la conformazione del volto mantengono una sostanziale stabilità, le qualità accidentali dipendono da variabili esterne e possono mutare in relazione a scelte personali o contingenze socio-economiche.

Il quarto e ultimo criterio si configura, infine, in relazione logico-strutturale con il primo, evidenziando una coerenza interna nel quadro normativo, ma al contempo segnando una discontinuità rispetto alla definizione adottata a livello internazionale dalla disciplina ISO/IEC 2382-37. Quest'ultimo, infatti, classifica i dati biometrici come informazioni potenzialmente impiegabili nei processi di riconoscimento individuale, senza tuttavia presupporre

---

[33] Rimane il fatto che «*biometric characteristics are not themselves considered biometric data. Only the personal data "resulting" from their processing qualify as biometric data. Thus, it is not the face of an individual, but the images of their face (pictures) that would be classified as biometric data. Likewise, it is not their fingertip, but a fingerprint image that will be classified as biometric data. As legally defined, "biometric data" are first of all "personal data". To be protected under data protection rules, personal data need to be, at least, part of a "filing system"or processed by automatic means. The biometric characteristics themselves cannot be processed. Only the data generated from these characteristics can*». Cfr. *Towards the European Level Exchange of Facial Images Legal Analysis for TELEFI project*, 7.2.2020. In letteratura cfr. E.J. KINDT, *Having yes, using no? About the new legal regime for biometric data*, cit., p. 11.

che essi siano necessariamente idonei a determinare in maniera autonoma l'identificazione univoca di un soggetto. In altre parole, gli standard internazionali sembrano adottare un approccio più neutro e tecnico, sottolineando la funzione probabilistica e contestuale del dato biometrico nel processo identificativo, piuttosto che attribuirgli un valore assoluto e deterministico.

La divergenza concettuale assume una particolare rilevanza nella distinzione tra il piano giuridico e quello scientifico-forense. Sotto il profilo normativo, affinché un dato rientri nella categoria ai sensi del GDPR, è necessario che esso sia in grado di consentire o confermare univocamente l'identità di una persona fisica [34]. L'impostazione presenta però criticità significative se analizzata dal punto di vista scientifico-forense. In ambito biometrico, la nozione di identificazione univoca presuppone il trattamento di un dato che, attraverso un processo di comparazione, consenta di attribuire un'identità a un soggetto. Nella pratica, tuttavia, la maggior parte dei sistemi di riconoscimento biometrico non fornisce risultati assoluti, bensì opera sulla base di probabilità statistiche, attribuendo un punteggio di similarità che quantifica il grado di corrispondenza tra un campione biometrico e i dati presenti in un database di riferimento [35]. Tale diversità di approccio risulta particolarmente evidente nei sistemi di riconoscimento facciale, nei quali il processo di comparazione biometrica tra un volto sconosciuto e un database di immagini preesistenti non produce un'identificazione diretta e univoca, bensì genera un insieme di possibili corrispondenze, ordinate in base a un indice di similarità probabilistica. Se, da un lato, in ambito normativo, il GDPR stabilisce che un dato personale deve consentire di stabilire o confermare l'identità di una persona fisica affinché sia qualificato come dato biometrico, dall'altro lato, in ambito scientifico-forense, l'identificazione biometrica non può mai essere considerata univoca e assoluta. La definizione presente nel regolamento e ripresa nella direttiva 2016/680/UE (LED), non troverebbe dunque riscontro scientifico [36]: sarebbe più opportuno esprimersi in termini di

---

[34] Cfr. E.J. KINDT, *Having yes, using no? About the new legal regime for biometric data*, cit., p. 12, «*governmental databases, collecting and keeping images of faces or fingerprints, for example collected for eID cards, do hence not fall under any specific biometric legislation if not used for identification purposes, other than the general data protection rules, as for all other personal data. There are hence no major restrictions or specific protection for such data collections. However, at the same time, such collections remain vulnerable for re-use, including biometric comparison and use for identification purposes*».

[35] Cfr. il capitolo II, § 4.

[36] Cfr. S. STALLA BOURDILLON, *The GDPR and The Biggest Mess of All: Why Accurate Legal Definitions Really Matter …*, 12 aprile 2016, https://peepbeep.wordpress.com/2016/04/12/the-gdpr-and-the-biggest-mess-of-all-why-accurate-legal-definitions-really-matter/.

probabilità di riconoscimento, o meglio, sarebbe più coerente riformulare la definizione come «*personal data relating to the physical, physiological or behavioural characteristics which can be used to recognize individuals to a certain degree of probability*»[37].

Questa riflessione sembra aver trovato, almeno in parte, un riscontro nel recente intervento normativo del legislatore europeo in occasione dell'introduzione del regolamento sull'intelligenza artificiale[38]. Tale atto fornisce una nuova definizione di dati biometrici, intesi come «dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici»[39].

L'eliminazione del criterio dell'univocità nella definizione normativa dei dati biometrici, però, non risponderebbe esclusivamente a un'esigenza di maggiore accuratezza scientifica, volta a riconoscere la natura probabilistica dei sistemi biometrici, ma rifletterebbe una scelta deliberata del legislatore europeo finalizzata a ricomprendere un più ampio spettro di trattamenti biometrici, che non si limitano alla mera identificazione personale[40]. Sebbene la nozione debba essere interpretata alla luce della normativa contenuta nel GDPR e nelle direttive di settore[41], tale impostazione estensiva potrebbe

---

[37] Cfr. *supra* la definizione ISO/IEC 2382–37:2022.

[38] Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, *COM/2021/206 final.*

[39] Art. 3, par. 1, n. 34.

[40] V'è da rilevare che, sia nella definizione di "*identificazione biometrica*" intesa come «il riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati», sia nella descrizione di un "*sistema di identificazione biometrica remota*" indicato come «un sistema di IA finalizzato all'identificazione di persone fisiche, senza il loro coinvolgimento attivo, tipicamente a distanza mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento» permane il medesimo scopo delle definizioni normative precedenti. Cfr. l'art. 3, par. 1, nn. 35 e 41 del regolamento sull'intelligenza artificiale.

[41] Cfr. il considerando 7, l'art. 3, par. 18, regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio del 23 ottobre 2018 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE, in *GUUE*, 21 novembre 2018, L 295/39; art. 3, par. 14, Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla

riflettere la volontà del legislatore europeo di ampliare il perimetro applicativo della disciplina, includendo non solo i sistemi di identificazione e autenticazione biometrica, ma anche tecnologie di categorizzazione biometrica e di analisi delle emozioni. Questi ultimi, pur non essendo finalizzati alla determinazione univoca dell'identità individuale, si basano comunque sull'elaborazione di caratteristiche biometriche per inferire attributi specifici, quali l'appartenenza a determinate categorie demografiche o tratti comportamentali, o per rilevare stati emotivi e reazioni psicofisiologiche [42].

Alla luce dell'analisi condotta, appare ragionevole interpretare il concetto di dato biometrico seguendo una prospettiva multifattoriale, che includa tanto il campione biometrico originario acquisito da un individuo, quanto la sua rappresentazione digitalizzata (*biometric sample*) o il modello biometrico elaborato a partire da esso [43]. Quest'ultimo, risultante dalla trasformazione

---

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. Trattandosi di dati particolarmente sensibili, in quanto idonei a identificare in modo univoco un individuo, l'art. 10 della direttiva (UE) 2016/680 ne assoggetta il trattamento da parte dalle autorità di *law enforcement* a criteri piuttosto stringenti. Esso è «autorizzato solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e soltanto: a) se autorizzato dal diritto dell'Unione o dello Stato membro; b) per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; c) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato». Il trattamento, anche automatizzato di dati biometrici intesi a identificare in modo univoco una persona è consentito a Europol dall'art. 30, par. 2, del regolamento (UE) 2016/794, come recentemente modificato dal regolamento (UE) 2022/991, con la «finalità di prevenire o combattere forme di criminalità organizzata nell'ambito degli obiettivi di Europol», ma pur sempre nel rispetto dei diritti e delle libertà dell'interessato attraverso le garanzie previste dallo stesso regolamento. Tale disposizione è stata introdotta in occasione della generale investitura conferita a Europol quale promotore dello sviluppo e della diffusione di un'intelligenza artificiale «etica, affidabile e antropocentrica, che è soggetta a solide garanzie in termini di protezione, sicurezza, trasparenza, spiegabilità e diritti» (considerando 49).

[42] Cfr. il capitolo II, § 4.5.1.

[43] In questo senso, cfr. Y. LIU, *Identifying Legal Concerns in the Biometric Context*, in *Journal of International Commercial Law and Technology*, 3(1), 2008 in cui si sottolinea che: «*the legal significance of biometric data*» include «*raw biometric images and biometric templates*»; cfr. anche A.I. AWAD-A.E. HASSANIEN, *Impact of Some Biometric Modalities on Forensic Science*, in A.K. MUDA *et al.* (a cura di), *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications*, in *Studies in Computational Intelligence* 555. S. SMYTH, nella sua recente ricerca "*Biometrics, surveillance and the law. Societies of restricted access, discipline and control*", Routledge, New York, 2019, p. 21, afferma che «*the term*

del dato grezzo mediante *specifici trattamenti tecnici*, consente la successiva elaborazione per finalità di identificazione o autenticazione. In tal senso, un dato biometrico può essere definito come un'informazione fisica, fisiologica o comportamentale che, una volta sottoposta a processi di elaborazione automatizzati, diviene suscettibile di utilizzo per operazioni di riconoscimento individuale, sia in modalità *one-to-one* (verifica) che *one-to-many* (identificazione) [44]. Un sistema di riconoscimento biometrico invece, deve essere inteso come qualsiasi strumento tecnologico in grado di effettuare l'identificazione o la verifica dell'identità di un individuo attraverso l'elaborazione automatizzata di caratteristiche biometriche, sulla base di trattamenti tecnici specifici. Tali sistemi operano mediante l'acquisizione, la normalizzazione, l'estrazione delle *features* biometriche e la successiva comparazione con dati già presenti in un archivio di riferimento.

Come visto, stabilire una definizione univoca di dato biometrico si è rivelata un'operazione alquanto complessa. Ciò è dovuto principalmente alla costante evoluzione del progresso scientifico e tecnologico che amplia le possibilità di acquisizione, elaborazione e conservazione dei dati biometrici, rendendo di fatto impossibile fornire un inquadramento statico e definitivo del fenomeno. La rapidità con cui si sviluppano nuove tecniche di riconoscimento – come l'integrazione di sistemi di intelligenza artificiale o l'analisi multimodale dei dati biometrici – impone un approccio dinamico e flessibile nella definizione normativa che possa adattarsi alle innovazioni senza cadere immediatamente nell'obsolescenza.

Inoltre, l'estensione delle applicazioni del riconoscimento biometrico al di fuori degli ambiti tradizionali della sicurezza e di *law enforcement* – ad esempio, nel settore commerciale, sanitario e dei servizi digitali – ha reso ancor più evidente la necessità di una definizione operativa capace di riflettere le diverse finalità d'uso. Se, infatti, nell'ambito della sicurezza il dato biometrico è trattato prevalentemente per finalità di identificazione e autenticazione, in altri contesti esso può essere utilizzato per scopi di categorizzazione, profilazione o analisi del comportamento, ampliando ulteriormente il perimetro delle questioni giuridiche ed etiche coinvolte. Di conseguenza, l'inquadramento del dato biometrico e dei sistemi di riconoscimento facciale deve necessariamente rifletterne la complessità

---

biometrics refers to the measurement of physical features of the human body. Put differently, biometrics is [also] the science of automatic identification or identity verification of individuals using [unique] physiological or behavioural characteristics».

[44] Cfr. *infra* il § 4.5.

interdisciplinare, evitando di adottare approcci rigidi che non siano in grado di intercettare le evoluzioni tecnologiche e i loro effetti sui diritti fondamentali [45].

3. *Le proprietà dei tratti biometrici e le classificazioni dei sistemi di riconoscimento*

Oltre che sulla marcata interdisciplinarità che caratterizza il ricorso ai dati biometrici, occorre soffermarsi anche sulla natura ibrida degli stessi, la quale impone un'analisi approfondita delle loro specifiche proprietà e delle dinamiche operative dei sistemi tecnologici deputati alla loro elaborazione.

Nella letteratura scientifica, è prassi consolidata distinguere i tratti biometrici in tre macro-categorie: fisici, fisiologici e comportamentali. Le caratteristiche fisiche comprendono quegli elementi strutturali del corpo umano tra i quali si annoverano le impronte digitali, l'iride, la retina, la geometria della mano, la conformazione dell'orecchio, l'odore corporeo e, naturalmente, la morfologia del volto. I dati biometrici di natura fisiologica si distinguono dai dati biometrici fisici in quanto fondati non già sull'analisi morfologica esterna degli individui, bensì sull'osservazione e misurazione delle funzioni biologiche interne e della biomeccanica corporea. Tali dati, pertanto, si riferiscono al funzionamento dinamico dell'organismo umano e si ottengono mediante la rilevazione di variabili corporee temporali, suscettibili di modificazione e di fluttuazione nel tempo. Esempi paradigmatici di questa categoria sono rappresentati dall'elettrocardiogramma (ECG), dai modelli di respirazione e dall'elettroencefalogramma (EEG), i quali forniscono una rappresentazione tracciabile e continuativa delle attività fisiologiche del soggetto. A differenza delle tecniche fondate sulla rilevazione di dati biometrici statici e istantanei, i sistemi basati su informazioni fisiologiche richiedono una osservazione prolungata e continuativa dell'individuo, così da cogliere le specifiche variazioni nel tempo di determinati parametri corporei.

Analogamente, i dati biometrici "comportamentali" richiedono

[45] Più ampiamente cfr. il capitolo III.

un'osservazione degli individui che introduce una variabile temporale nella valutazione. Tra le caratteristiche "comportamentali" si annoverano la scrittura, la battitura sulla tastiera, la cadenza dell'andatura e la voce [46].

Le caratteristiche biometriche vengono generalmente analizzate e valutate sulla base di parametri oggettivi, i quali ne determinano l'idoneità all'impiego nei diversi contesti applicativi. La loro misurabilità secondo criteri standardizzati consente infatti di stabilire dal punto di vista tecnico il grado di affidabilità, precisione e adattabilità ai sistemi di riconoscimento automatizzato [47].

La prima proprietà è l'*universalità*, intesa come la diffusione della caratteristica biometrica nella popolazione umana. Affinché un tratto fisiologico o comportamentale possa essere impiegato in modo efficace per finalità identificative, è necessario che esso sia presente in tutti gli individui, senza eccezioni, o quantomeno in una percentuale statisticamente significativa, tale da garantirne l'applicabilità su larga scala.

Il secondo criterio è rappresentato dall'*unicità* o *singolarità*, ossia la capacità della caratteristica biometrica di essere univocamente associata a un solo individuo. Tale qualità, nota anche come *riferibilità individualizzante* o *distintività*, è fondamentale affinché il sistema riesca a distinguere un soggetto da tutti gli altri, minimizzando i rischi di sovrapposizione tra profili biometrici "simili". È opportuno evidenziare che la singolarità del tratto biometrico non costituisce una qualità assoluta e invariabile, ma va contestualizzata in relazione al sistema impiegato, alla risoluzione dell'immagine acquisita, nonché alla quantità di dati archiviati nella banca dati di riferimento. All'aumentare della dimensione del database, infatti, cresce anche la probabilità di sovrapposizioni statistiche tra profili con elevato grado di somiglianza morfologica, con conseguente incremento dell'errore identificativo.

Un ulteriore criterio fondamentale nella valutazione delle caratteristiche

---

[46] Cfr. B. LAVANYA-H.H. INBARANI, *A Survey of Biometric Techniques*, in *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(7), 2015 in cui si afferma che «*dynamic signature verification, keystroke dynamics and speaker verifications are examples of behavioral characteristics. Physiological characteristics include hand or finger recognition, facial characteristics, and iris recognition*».

[47] Per un approfondimento sul tema cfr. J. WAYMAN, *Biometric Systems, Technology, Design and Performance Evaluation*, Springer, London, 2004 e G. IOVANE, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza*, Aracne, Roma, 2008, p. 173.

biometriche è rappresentato dall'*invariabilità*, intesa come la stabilità della caratteristica nel tempo. Affinché un tratto biometrico possa essere sfruttato nel tempo, è necessario che esso rimanga costante e immune da variazioni significative, indipendentemente da fattori esterni o condizioni contingenti. L'efficienza dei sistemi di riconoscimento biometrico si basa principalmente sulla possibilità di confrontare i dati acquisiti con quelli precedentemente archiviati, presupponendo che la caratteristica analizzata non subisca mutamenti repentini tali da comprometterne la riconoscibilità. In altre parole, la capacità di un sistema biometrico di generare risultati coerenti e affidabili dipende dall'immutabilità relativa del tratto analizzato, ossia dalla sua resistenza a fenomeni di alterazione dovuti all'invecchiamento, a modificazioni fisiologiche o a interferenze ambientali.

L'*accettabilità* rappresenta invece un parametro essenziale nella valutazione dell'idoneità operativa dei sistemi biometrici, in quanto attiene al grado di intrusività della procedura di acquisizione rispetto all'integrità fisica e alla sfera individuale della persona. Affinché un sistema biometrico possa essere implementato su larga scala, esso deve essere progettato in modo da minimizzare qualsiasi forma di disagio o danno per l'individuo, garantendo al contempo un livello di sicurezza e affidabilità compatibile con i principi di proporzionalità e tutela dei diritti fondamentali [48]. L'*accettabilità* di una tecnologia biometrica non si limita esclusivamente agli aspetti tecnici, ma comprende anche una dimensione sociale, che implica la necessità di valutare il grado di percezione pubblica della tecnologia in questione. Un sistema biometrico può dirsi efficace e sostenibile solo se risulta socialmente accettabile per una parte significativa della popolazione, evitando forme di coercizione implicita o resistenza diffusa, legate a timori di violazione della privacy, uso improprio dei dati personali o sorveglianza pervasiva.

Strettamente correlato è il parametro dell'*acquisibilità* che si riferisce alla possibilità di raccogliere il dato biometrico in tempi più o meno ragionevoli e senza complicazioni operative. Per garantire l'efficienza dei sistemi biometrici, la procedura di rilevamento deve essere rapida, semplice ed eseguibile in qualsiasi condizione ambientale, evitando che fattori esterni possano compromettere la qualità del dato raccolto.

Ulteriore caratteristica è la *riducibilità* o *collezionabilità*, ossia la capacità della caratteristica biometrica di essere quantificabile e inserita in un sistema di archiviazione standardizzato. La misurabilità del dato è

[48] Cfr. il capitolo III, § 4 ss.

essenziale affinché esso possa essere elaborato da algoritmi di riconoscimento, normalizzato in formati interoperabili e memorizzato in database strutturati per la consultazione e il confronto con altre informazioni biometriche.

Infine, il *gradimento* esprime il livello di accettazione della tecnologia da parte dell'utente finale. Sebbene tale criterio possa sembrare secondario rispetto ad altri parametri di natura tecnica, esso assume rilevanza in quanto un sistema di identificazione biometrico, per essere adottato con successo, deve ottenere la fiducia degli utenti e risultare intuitivo.

Talune caratteristiche individuali, sebbene dotate del requisito di *universalità* – come ad esempio il peso corporeo, il colore degli occhi e dei capelli – non vengono generalmente incluse, secondo l'impostazione scientifica prevalente, nella categoria dei dati biometrici in senso proprio. Ciò in quanto tali tratti, pur essendo potenzialmente comuni a ogni individuo, non soddisfano congiuntamente gli ulteriori requisiti richiesti per l'inquadramento nella definizione di dato biometrico, quali la *permanenza* o la *distintività*[49]. Ad esempio, alcune di queste caratteristiche – come il peso – non presentano una *riferibilità individualizzante* sufficiente da consentire la distinzione inequivocabile di un individuo rispetto a un altro all'interno di una determinata popolazione[50].

La tabella seguente riporta una classificazione esemplificativa di alcuni tratti biometrici in base all'*invariabilità*, alla *singolarità* e all'*accettabilità*[51].

---

[49] Nei casi citati, la singolarità, la misurabilità o l'invariabilità. Cfr. G. IOVANE, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza*, cit., p. 173.

[50] Tali dati rientrano nella categoria dei cd. "*soft biometric data*". A. DANTCHEVA-C. VELARDO-A. D'ANGELO-J.L. DUGELAY, *Bag of Soft Biometrics for Person Identification: new trends and challenges*, in *Multimedia Tools and Application*s, 51(2), 2010, p. 739-777; A.K. JAIN-S.C. DASS-K. NANDAKUMAR, *Soft biometric traits for personal recognition systems* in *International Conference on Biometric Authentication*, 2004.

[51] La tabella è basata sui dati tratti da G. IOVANE, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza*, cit., p. 172.

Tabella 1: *classificazione di alcuni tratti biometrici e indici di invariabilità, singolarità e accettabilità*

Caratteristiche	Tecnologia di acquisizione	Invariabilità	Singolarità	Accettabilità
Geometria della mano	Ottica (IR)	Buona	1:1000	Molto buona
Geometria della dita	Ottica (IR)	Buona	1:1000	Molto buona
Retina	Ottica	Molto buona	1:10 Milioni	Non buona
Iride dell'occhio	Ottica	Molto buona	1:6 Milioni	Buona
Vene superficiali della mano	Ottica (IR)	Buona	Non nota	Molto buona
Firma	Dinamica (pressione)	Non buona	1:1000	Molto buona
Voce	Elettroacustica	Non buona	1:1000	Buona
Volto	Ottica o IR	Buona	Dipendente dal sistema	Buona
Impronta digitale	Ottica, Capacitiva etc..	Molto buona	1:10 Milioni	Buona

Ulteriori distinzioni riguardano più specificamente gli strumenti impiegati per eseguire le comparazioni[52]. La classificazione dei sistemi di riconoscimento si fonda su variabili di carattere tecnico e ambientale, che influenzano il grado di affidabilità e la precisione dei risultati[53]. Un sistema biometrico si compone generalmente di tre elementi fondamentali: un modulo di acquisizione dei dati biometrici, che può consistere in dispositivi *hardware* quali telecamere, scanner o sensori dedicati; un software di elaborazione e mappatura biometrica, responsabile dell'estrazione delle *features* distintive del dato grezzo e della loro successiva digitalizzazione; e infine, una banca dati per la registrazione e la memorizzazione delle informazioni, destinata a essere utilizzata per il confronto con i dati acquisiti.

I sistemi di riconoscimento biometrico possono essere classificati secondo diverse categorie, in base alle loro modalità di funzionamento e alle condizioni in cui operano. Un primo criterio di distinzione riguarda l'esteriorità del sistema, che può essere *manifesto* o *occulto,* a seconda che l'utente sia consapevole o meno di essere sottoposto a un processo di riconoscimento

[52] Cfr. J. WAYMAN, *Biometric Systems, Technology, Design and Performance Evaluation*, Springer, London, 2004.

[53] Cfr. il capitolo II, § 4.6.

biometrico. Naturalmente, la scelta di adottare una specifica tipologia di sistema di riconoscimento è strettamente correlata alle finalità operative che si intendono perseguire. In ambito privato, la maggior parte dei sistemi di identificazione biometrica opera in modalità *manifesta*, per finalità di autenticazione e controllo degli accessi a determinati luoghi fisici. Tali sistemi sono progettati per garantire agli utenti un livello adeguato di trasparenza, consentendo loro di essere pienamente consapevoli del trattamento dei propri dati biometrici. Al contrario, nell'ambito della sicurezza pubblica e delle attività di *law enforcement*, l'impiego di sistemi di riconoscimento biometrico avviene frequentemente in modalità *occulta*, al fine di ottimizzare le operazioni di identificazione, senza interferire con il comportamento dei soggetti sottoposti a controllo.

Nella disciplina biometrica, si è soliti suddividere i sistemi anche in base al tipo di *accesso* da eseguire[54]. Nei sistemi di *accesso fisico*, il controllo biometrico è finalizzato a monitorare, limitare o autorizzare il movimento di persone in determinati spazi fisici, come edifici o locali riservati, nonché ad abilitare l'utilizzo di specifiche attrezzature o dispositivi. Nei sistemi di *accesso logico*, invece, il riconoscimento biometrico è impiegato per autenticare l'identità dell'utente e consentire l'accesso a dati, risorse digitali o infrastrutture informatiche, configurandosi, dunque, come un meccanismo di protezione dei sistemi informativi e dei dati ivi contenuti.

Un'altra distinzione riguarda le tempistiche del procedimento. I sistemi possono operare riconoscimenti *contestuali* o *differiti*, a seconda che il confronto tra il dato acquisito e quello contenuto nella banca dati avvenga *in tempo reale* o con un ritardo significativo rispetto alla fase di acquisizione. I sistemi contestuali sono generalmente utilizzati in scenari di sicurezza pubblica, come quelli che sfruttano il riconoscimento facciale nei flussi di sorveglianza, mentre quelli differiti sono impiegati per analisi post-evento, ad esempio nell'elaborazione forense di immagini e video raccolti da telecamere di videosorveglianza.

Dal punto di vista operativo, i sistemi possono essere *presidiati* o non *presidiati*, a seconda che il processo di riconoscimento sia supervisionato da un operatore umano o sia interamente automatizzato. Nei sistemi presidiati, un intervento umano è richiesto per validare o correggere i risultati generati

---

[54] Cfr. S. NANAVATI-M. THIEME-R. NANAVATI, *Biometrics. Identity verification in a networked world*, Wiley Computer Publishing, New York, 2002, p. 14-15; A.K. JAIN-A. ROSS-S. PRABHAKAR, *An Introduction to Biometric Recognition*, in *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 2004, p. 13.

dall'algoritmo, riducendo il rischio di falsi positivi o negativi, mentre nei sistemi non presidiati il riconoscimento avviene senza alcuna supervisione diretta, aumentando l'autonomia del processo, ma riducendo le possibilità di controllo immediato sugli esiti.

Un'ulteriore classificazione viene eseguita in base alle condizioni ambientali. I sistemi possono essere progettati per funzionare in condizioni standard, con parametri di temperatura, umidità e illuminazione ottimali, oppure possono essere adattati a scenari operativi critici, come ambienti scarsamente illuminati o con elevata variabilità delle condizioni atmosferiche, situazioni che possono influenzare la qualità della rilevazione biometrica e aumentare il tasso di errore.

Infine, i sistemi possono essere *cooperativi* o *non cooperativi*, a seconda che richiedano la collaborazione attiva dell'individuo sottoposto al riconoscimento (ad esempio, la scansione volontaria delle impronte digitali o la posa per il riconoscimento facciale) o che operino in modo autonomo, senza necessità di un'azione consapevole da parte del soggetto identificato.

L'eterogeneità delle classificazioni applicabili ai sistemi biometrici evidenzia, in maniera inequivocabile, la complessità strutturale e la versatilità funzionale che connotano tali tecnologie. Le diverse modalità di implementazione e le variegate finalità di utilizzo, che possono spaziare dalla semplice autenticazione personale fino al riconoscimento massivo a distanza, impongono una valutazione puntuale e contestualizzata dell'impiego di ciascun metodo di riconoscimento, tenendo conto delle specifiche esigenze operative e del contesto normativo e sociale in cui esso si inserisce.

In questo scenario, la selezione del sistema più idoneo non può essere frutto di una scelta meramente tecnica, ma deve fondarsi su un'analisi multilivello che tenga in considerazione, da un lato, il grado di accuratezza e affidabilità richiesto dall'ambito applicativo e, dall'altro, il livello di accettabilità sociale e percezione pubblica della tecnologia in questione.

4. *Il funzionamento tecnico della tecnologia di riconoscimento facciale*

Operati gli inquadramenti necessari riguardanti la disciplina scientifica di riferimento, è ora possibile concentrare l'analisi sull'*iter* procedurale e

sulle metodologie operative che caratterizzano più specificamente il procedimento di riconoscimento facciale.

L'elaborazione automatizzata delle immagini digitali si articola in una sequenza strutturata di fasi, ciascuna delle quali è funzionalmente orientata al perseguimento di specifiche finalità predeterminate. L'impiego di questa tecnologia può avvenire infatti per finalità identificative, autenticative o di categorizzazione[55], tramite la comparazione di immagini digitali o di modelli elettronici (cd. *template*), ossia rappresentazioni vettoriali delle caratteristiche distintive di uno specifico tratto fisico considerato[56]. Da una fotografia o da un video ritraente un soggetto, è possibile ricavare l'insieme delle *features* (o cd. *punti di repere*)[57], generando il cd. "modello elettronico" di quello specifico tratto biometrico[58], il quale sarà oggetto di una successiva comparazione automatizzata con un altro *template* o rappresentazione digitalizzata precedentemente registrata.

Tramite alcune semplificazioni, è possibile immaginare un vero e proprio *ciclo del dato biometrico* che, dall'acquisizione del campione grezzo, conduce alla rappresentazione dell'immagine digitalizzata o del "corpo elettronico". Bisogna però segnalare che le fasi del procedimento variano a seconda delle finalità applicative che si intendono raggiungere. Risulta comunque possibile,

---

[55] Su queste ci si soffermerà meglio più avanti, cfr. *infra* il § 4.5.

[56] Per un primo approfondimento cfr. S. AMATO-F. CRISTOFARI-S. RACITI, *Biometria. I codici a barre del corpo*, Giappichelli, Torino, 2013, p. 33; EUROPEAN PARLIAMENT, *Regulating facial recognition in the EU*, EPRS | European Parliamentary Research Service, 2021; WORLD ECONOMIC FORUM, *A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations*, 2021; INFORMATION COMMISSIONER'S OPINION, *The use of live facial recognition technology in public places*, 18 giugno 2021, p. 4, https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf.

[57] «I principali *punti di repere* sono: il *nasion* (radice del naso); *glabella* (punto situato al di sopra della radice del naso, dove la cute è in genere priva di peluria); *pronasale* (punto più sporgente della punta del naso); *naso spinale* (punto corrispondente al sottosetto nasale); *alare* (punto più sporgente dell'ala del naso); *prosthion* (punto superiore del solco naso labiale); *gonion* (margine inferiore del ramo della mandibola); *gnathion* (sporgenza inferiore del mento); *trichion* (punto di attacco dei capelli sulla fronte); *vertex* (punto più alto del cranio); *zygion* (punto più sporgente dello zigomo)». N. BALOSSINO-S. SIRACUSA, *L'identificazione basata sul volto: metodi fisionomici e metrici*, Security Forum, Edizioni ItasForum, Bergamo, 2004, p. 4.

[58] Il "modello elettronico" o "*biometric template*" può essere definito come l'«insieme di tratti biometrici memorizzati informaticamente e direttamente confrontabile con altri modelli biometrici». *Linee-guida in materia di riconoscimenti biometrico e firma grafometrica. Allegato A al Provvedimento del Garante del 23 novembre 2014*, 12 novembre 2014, p. 5.

in linea generale e pur nella diversità e complessità delle più o meno avanzate tecnologie di riconoscimento adottate, distinguere e schematizzare il percorso, seguendo una determinata sequenza di fasi [59].

Il primo momento coincide con l'*acquisizione* (o *enrollment*) della rappresentazione digitalizzata dell'immagine di un volto: quest'ultima può trovarsi sotto forma di fotografia analogica o digitale, ovvero "ritagliata" come *frame* da una videoregistrazione. Tale fase può essere condotta in un ambiente controllato, attraverso sistemi biometrici partecipativi, laddove si preveda la cooperazione dell'interessato durante il momento di raccolta del dato biometrico, ovvero in ambienti "non controllati", tramite sistemi "passivi", senza che l'interessato ne abbia piena consapevolezza [60].

La seconda fase è quella di *individuazione* di uno o più volti (cd. "*face detection*") [61]. Trattasi del momento in cui «si isola, all'interno dell'immagine, la presenza di un volto rispetto allo sfondo; operazione che può essere anche molto complessa soprattutto nei sistemi biometrici passivi» [62]. In questi casi, fattori come l'illuminazione ambientale, l'angolazione del volto, la presenza di occlusioni parziali (ad esempio, occhiali, mascherine o copricapi) e la qualità dell'immagine possono influenzare significativamente la capacità del sistema di individuare correttamente i volti [63].

Nei contesti in cui la rilevazione biometrica avviene *in tempo reale*, attraverso flussi video, come nelle reti di videosorveglianza pubblica, la fase di *face detection* assume un ruolo di primaria rilevanza operativa. Tale processo deve essere eseguito con elevata rapidità ed efficienza, al fine di garantire un'analisi tempestiva e accurata delle immagini acquisite, condizione indispensabile per l'efficacia del sistema. La fase di individuazione rappresenta il passaggio preliminare essenziale affinché il sistema possa successivamente procedere alla comparazione biometrica, confrontando i volti rilevati con quelli presenti nei database di riferimento.

---

[59] Cfr. S.Z. LI-A.K. JAIN, *Handbook of Face Recognition*, Springer, New York, 2011, p. 3 ss. e C. GARVIE-A. BEDOYA-J. FRANKLE, *The perpetual line-up: Unregulated police face recognition in America*, cit., p. 9.

[60] *Linee-guida in materia di riconoscimenti biometrico e firma grafometrica. Allegato A al Provvedimento del Garante del 23 novembre 2014*, 12 novembre 2014, p. 6.

[61] Cfr. V. MANFREDI-E. PESSA, *Il riconoscimento dei volti: aspetti cognitivi, neuropsicologici e computazionali*, in *Sist. intell.*, 3, 2011, p. 456.

[62] Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 32.

[63] Cfr. *infra* il § 4.6.

Segue, poi, la cd. *normalizzazione*, ossia il procedimento di modifica e attenuazione delle variazioni del volto dovute alla posa, ovvero alla scarsa o eccessiva illuminazione dell'immagine. Durante questa operazione è già possibile individuare le specifiche caratteristiche distintive del volto, quali la posizione degli occhi, del naso, della bocca e di altri elementi facciali rilevanti per il riconoscimento biometrico. L'efficacia della normalizzazione incide direttamente sulle prestazioni complessive del sistema, in quanto un'elaborazione non ottimale può influenzare la precisione delle fasi successive, aumentando il rischio di falsi positivi o negativi [64].

Si prosegue con il momento di *estrazione* delle caratteristiche. L'insieme dei tratti fondamentali del volto può essere convertito nel suo *template*, o modello elettronico corrispondente, analogamente a quanto avviene per altri dati biometrici grezzi, al fine di comparare lo stesso con altri *templates p*resenti all'interno di una banca dati. Trattasi di uno stadio solamente "eventuale" dal momento che le più moderne tecniche di intelligenza artificiale, durante l'apprendimento e l'analisi della rappresentazione digitalizzata del volto, permettono di ricavare le *features* tipiche, automaticamente, senza che l'estrazione delle stesse costituisca un momento a sé stante [65]. L'evoluzione della tecnologia basata sull'intelligenza artificiale ha infatti permesso di ottimizzare i processi di identificazione, rendendo possibile l'estrazione automatizzata delle *features* biometriche direttamente dall'immagine digitalizzata, senza la necessità di un'ulteriore fase di pre-elaborazione manuale o di conversione in *template.*

A questo punto, si giunge alla fase di *registrazione* e successiva *conservazione* della rappresentazione digitale dell'immagine, ovvero del suo modello elettronico, all'interno di un database per il successivo momento di *confronto* (o cd. *biometric match*) [66]. Quest'ultimo costituisce lo snodo principale

---

[64] Cfr. *infra* il § 4.6.

[65] «L'estrazione delle caratteristiche può essere olistica, intesa come rappresentazione matematica dell'intera immagine facciale, come risulta dall'analisi dei suoi principali componenti; o basata sui singoli tratti biometrici, quale rappresentazione digitalizzata solamente di alcune specifiche caratteristiche localizzate del volto; o una combinazione dei due metodi (metodo di estrazione ibrido delle caratteristiche)». G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 33.

[66] Cfr. G. FORMICI, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i legislatori e le Corti*, in *Saggi – DPCE online*, 2, 2019, p. 1111; J.N. PATO, L. I. MILLETT, *Biometric Recognition: Challenges and Opportunities*, in *The National Academies Press*, su http://www.nap.edu/catalog.php?record_id=12720, p. 2 e A. JAIN-R. BOLLE-S. PANKANTI, *Biometrics. Personal identification in Networked Society*, Springer Science, New York, 1999, p. 28.

di tutto il procedimento di riconoscimento facciale, dal momento che è in tale fase che avviene la *misurazione* e la *comparazione* delle somiglianze tra le caratteristiche e i tratti biometrici di un modello elettronico e altri dati già registrati in un archivio di riferimento.

Al livello di somiglianza e correlazione viene assegnato un punteggio valutato rispetto ad una soglia predefinita [67]. Se il risultato eccede quest'ultimo valore, si determina una combinazione e, dunque, il soggetto viene "riconosciuto"; in caso contrario, non avrà luogo alcun *match* (cd. *non-match*) [68]. Tale operazione è realizzata attraverso algoritmi di comparazione che analizzano la corrispondenza tra i *punti di repere* precedentemente individuati e i dati biometrici disponibili, determinando un indice di similarità che stabilisce la probabilità di un'identificazione corretta. La precisione di questa fase è influenzata da molteplici fattori, tra cui la qualità delle immagini raccolte, le capacità computazionali del sistema e l'eventuale presenza di *bias* algoritmici che possono alterare l'accuratezza del risultato [69].

Le modalità applicative dei sistemi di riconoscimento facciale sono essenzialmente due [70]. La prima *contestuale, dal vivo* o *in tempo reale* [71], consente il riconoscimento senza ritardo o con un ritardo non significativo rispetto al momento di acquisizione del dato, in un'area geografica delimitata, attraverso flussi di dati provenienti, per esempio, da telecamere ivi

---

[67] Tale valore minimo viene generalmente stabilito dall'amministratore del sistema cosicché, a seconda del grado di sicurezza desiderato, è possibile optare per sistemi con soglie più o meno elevate. «*Matching is a probabilistic process, as the system expresses the similarity of the images with a percentage value, called a "similarity score"*». G. MOBILIO, *Your face is not new to me – Regulating the surveillance power of facial recognition technologies*, in *Int. Pol. Rev.*, 12(1), 2023.

[68] «In funzione del superamento di una soglia prestabilita, il sistema può validare una "verifica di identità" oppure, in modalità identificazione, generare una lista di possibili candidati caratterizzati da un punteggio di "accoppiamento" (*matching*); il sistema attribuisce alla persona oggetto della transazione l'identità del candidato con il migliore punteggio di "accoppiamento"». COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, 26 novembre 2020. Sia consentito il rinvio anche a E. SACCHETTO, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Dir. pen. cont.-Riv. trim.*, 2, 2019, p. 469.

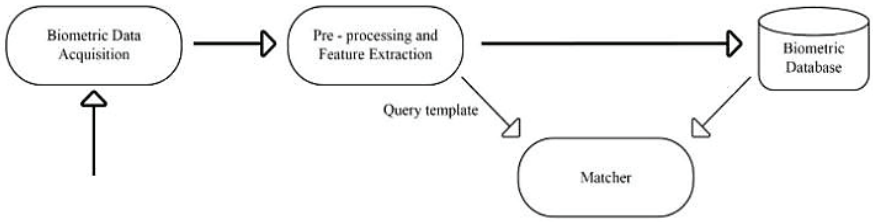
[69] Cfr. il capitolo II, § 4.6.

[70] La distinzione coincide pressoché con le differenze descritte per le modalità *real-time* ed *enterprise* del software SARI. Cfr. il § 4.1.

[71] O in *real time.*

installate [72]. Questa modalità consente di monitorare specifiche aree, al fine di prevenire, ad esempio, un potenziale pericolo di attentati o una minaccia per l'ordine pubblico (es. stadi, aeroporti, ecc.). Il software è in grado di collezionare le rappresentazioni digitalizzate di dati biometrici di un numero indeterminato di individui [73], potendo altresì eseguire eventuali comparazioni con un gruppo preselezionato di immagini acquisite e, in alcuni casi, conservarle per eventuali futuri *matches* [74]. Il sistema compara, infatti, i volti nei flussi video con quelli presenti all'interno di una banca dati predefinita e, in caso di *match* fra due rappresentazioni digitali, il sistema genera un *alert c*he restituisce un risultato di compatibilità espresso in percentuale [75].

Schema 1: *procedimento in modalità 1:N, 1:N+1 e 1:1*



La seconda modalità operativa del riconoscimento facciale è quella *statica*, *a posteriori* o *post remote*, caratterizzata dal fatto che i dati biometrici vengono acquisiti in un momento antecedente rispetto alla fase di confronto, il quale avviene con un ritardo significativo rispetto all'acquisizione dell'immagine. In questo caso, il materiale analizzato – costituito da immagini o

[72] Cfr. J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del Garante Privacy D'Oltremanica)*, in *Sist. pen.*, 28 marzo 2020, p. 3.

[73] Cfr. INFORMATION COMMISSIONER'S OPINION, *The use of live facial recognition technology in public places*, 18.6.2021, p. 4, reperibile su https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf.

[74] Cfr. E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Dir. pen. uomo*, 19 maggio 2021, p. 5.

[75] Cfr. INFORMATION COMMISSIONER'S OPINION, *The use of live facial recognition technology in public places*, 18 giugno 2021, cit., p. 14.

filmati raccolti da sistemi di videosorveglianza, come le telecamere a circuito chiuso (CCTV) – è stato generato prima che il sistema venga utilizzato per identificare un soggetto specifico, distinguendosi così dal riconoscimento eseguito *in tempo reale.* Il funzionamento di questa modalità si basa su un meccanismo di ricerca automatizzata all'interno di una banca dati preesistente, attraverso il quale il sistema individua e restituisce una lista di profili corrispondenti, ordinati in base al grado di similarità biometrica tra il volto analizzato e quelli già archiviati nel database. L'affidabilità di tale operazione dipende in gran parte dalla qualità delle immagini acquisite e dalla capacità dei modelli di elaborazione di distinguere con precisione i tratti biometrici, evitando errori di identificazione dovuti a variazioni dell'angolazione del volto, condizioni di illuminazione non ottimali o distorsioni derivanti dal processo di digitalizzazione[76]. Un aspetto peculiare di questa modalità è la possibilità, per l'operatore che utilizza il software, di affinare i risultati della ricerca mediante l'applicazione di filtri specifici. Questi consentono di restringere l'ambito dell'analisi a una determinata porzione del database, sulla base di informazioni anagrafiche o descrittive associate alle immagini archiviate. Tra i parametri comunemente impiegati figurano il sesso, il colore della pelle, l'altezza e la presenza di segni distintivi (ad esempio, cicatrici o tatuaggi). Sebbene tale funzione possa contribuire a incrementare l'efficienza del sistema, essa solleva al contempo rilevanti questioni etiche e giuridiche, in particolare per quanto concerne il rischio di discriminazioni basate su caratteristiche somatiche e l'eventuale rafforzamento di *bias* algoritmici preesistenti[77].

L'ambito fin qui esaminato rientra nella più ampia categoria dell'analisi facciale, un concetto che comprende un insieme eterogeneo di tecniche avanzate di elaborazione delle immagini biometriche. Queste metodologie sono finalizzate all'estrazione e all'analisi di specifiche caratteristiche morfologiche del volto, senza necessariamente comportare un'identificazione dell'individuo. L'analisi facciale, infatti, può essere impiegata per scopi differenti rispetto al riconoscimento biometrico in senso stretto, come il rilevamento dell'età, l'analisi delle espressioni facciali per la valutazione di stati emotivi o l'individuazione di parametri utili per la categorizzazione dei soggetti in base a determinati attributi. Come si vedrà a breve[78], questo può

[76] Cfr. più ampiamente il § 4.6.

[77] Si rimanda al § 4.6.

[78] Cfr. § 4.5.

avvenire suddividendo gli elementi distintivi del volto in categorie qualitative, ad esempio "genere" o "origine etnica", oppure effettuando stime quantitative per aspetti che possono essere rappresentati numericamente, come l'età.

Quello descritto è il generale funzionamento del procedimento di riconoscimento facciale. Vale la pena ora proseguire concentrando l'attenzione su un caso di studio specifico, il SARI, strumento attualmente impiegato dalle forze di polizia italiane in supporto alle attività investigative.

4.1. *Le peculiarità del Sistema Automatico di Riconoscimento delle Immagini (SARI): contesto di riferimento e dettagli operativi*

Sul piano nazionale, i primi passi operativi in materia sono stati compiuti dal Ministero dell'Interno, nel cui ambito, nel 2016, è stata avviata una procedura a evidenza pubblica per dotare le forze di polizia di un'infrastruttura informatica denominata "*Sistema Automatico Riconoscimento Immagini*", conosciuta ai più con il suo acronimo "SARI" [79].

[79] Da qui in avanti "SARI". Per un approfondimento sul tema cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, p. 240 ss.; E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, cit., p. 16 ss.; R. LOPEZ, *La rappresentazione facciale tramite software*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2019, p. 241 ss.; R. LOPEZ, *Riconoscimento facciale tramite software e individuazione del sospettato*, in A. SCALFATI (a cura di), *Pre-investigazioni (Espedienti e mezzi)*, Giappichelli, Torino, 2020, p. 297 ss.; J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del Garante Privacy D'Oltremanica)*, in *Sist. pen.*, 28 marzo 2020, p. 241 ss.; R.V.O. VALLI, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, in *Il Penalista*, 16 gennaio 2019; S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, 2020, p. 66 ss. e A. FONSI, *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time*, in *Riv. pen. dir. e proc.*, 13 maggio 2021. Sia consentito il richiamo a E. SACCHETTO, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *Leg. pen.*, 16 ottobre 2020; E. SACCHETTO, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Dir. pen. cont.-Riv. trim.*, 2, 2019; E. SACCHETTO, *Biometrics as forensic evidence: some reflections from the Italian Criminal proceeding's point of view, 8th International Workshop on Biometrics and Forensics* (IWBF), 2020; E. SACCHETTO, *Brevi riflessioni sui fondamenti e sui limiti del rapporto fra automated faced-based human recognition technology e processo penale*, in *ASTRID*, 4/2023 e E. SACCHETTO, *Automated faced-based human*

Un tentativo di ricostruzione delle caratteristiche costitutive e operative di questo «nuovo e, per certi versi, rivoluzionario»[80] strumento, può essere esperito attraverso il capitolato tecnico[81] allegato al contratto che il Ministero ha sottoscritto con l'azienda privata fornitrice del software[82]. Come specificamente richiesto dal committente, lo strumento è stato predisposto in modo da gestire due scenari operativi, "*enterprise*" e "*real-time*", coincidenti con le due finalità applicative tipiche di questi strumenti[83]. Per mezzo della prima, in uso dal settembre 2018, l'operatore confronta il volto del destinatario con quelli presenti all'interno della banca dati AFIS-SSA (*Automated fingerprint identification system*)[84], alla ricerca di un *match.* Al termine del processo di elaborazione, l'algoritmo di riconoscimento biometrico produce, come già anticipato, un elenco di profili potenzialmente corrispondenti, ordinati sulla base di un punteggio di probabilità che quantifica il grado di similarità tra l'immagine analizzata e quelle presenti nel database di riferimento. Tale punteggio è il risultato di un complesso calcolo algoritmico che tiene conto di vari parametri biometrici, tra cui la distanza relativa tra i *punti di repere* del volto, le caratteristiche morfologiche e altre metriche estratte durante la fase di elaborazione

---

recognition technologies e procedimento penale alla luce della proposta di regolamento sull'IA: alcuni spunti di riflessione, in C. CAMARDI (a cura di), *Collana del Centro Studi Giuridici del Dipartimento di Economia di Ca' Foscari, atti del Convegno "La via europea per l'intelligenza artificiale"*, Venezia il 25-26 novembre 2021, Wolters Kluwer Cedam, Milano, 2023.

[80] L'espressione è di R. LOPEZ, *La rappresentazione facciale tramite software*, cit., p. 241.

[81] Cfr. MINISTERO DELL'INTERNO – DIPARTIMENTO DI PUBBLICA SICUREZZA, *Capitolato tecnico, Procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini (S.a.r.i.) lotto n° 1*, reperibile su https://www.poliziadistato.it/statics/06/20160627-ctsari%2D%2D4-.pdf.

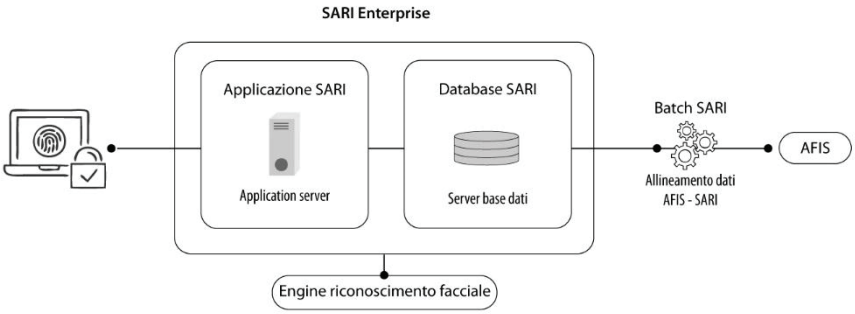
[82] L'azienda privata Parsec 3.26 S.r.l. opera nel settore dell'intelligenza artificiale e collabora con l'Istituto di Scienze Applicate e Sistemi Intelligenti del Consiglio Nazionale delle Ricerche (CNR), cfr. https://www.parsec326.it/.

[83] Attualmente, non si dispone di fonti ufficiali o documentazione certa riguardante l'implementazione del sistema SARI 2.0, né risultano dichiarazioni istituzionali che ne confermino l'operatività o l'effettiva adozione. L'ultima informazione reperibile, pubblicata sul sito web dell'Arma dei Carabinieri e risalente ad agosto 2024, fa riferimento a un capitolato tecnico che descrive in termini generici un dispositivo installato su piattaforme mobili. Secondo tale documento, lo strumento in questione sembrerebbe dotato di funzionalità avanzate, tra cui la capacità di analizzare e riconoscere il contenuto di chat, identificare gli account utente impiegati, rilevare il numero di conversazioni avvenute e implementare sistemi di biometria vocale. Cfr. https://www.carabinieri.it/in-vostro-aiuto/amm-trasp/gare-appalto/gare-appalto/cums_99_87_2024.

[84] Da qui in avanti AFIS. Più ampiamente, cfr. il § 4.2.

dell'immagine. Nel caso in cui venga rilevata una corrispondenza con un volto archiviato, il sistema genera automaticamente, come ormai noto, un segnale di *alert*, notificando all'operatore un *match.*

Figura 1: *architettura logica di SARI Enterprise*



Viceversa, la modalità *real-time* permette l'analisi automatica *in tempo reale* di soggetti ripresi in più flussi video provenienti dalle telecamere installate nella medesima area geografica. Il funzionamento di tale sistema si basa su un processo di elaborazione avanzato [85], che consente di estrarre e confrontare i volti presenti nei fotogrammi (*frame*) acquisiti dai flussi video [86]. Lo strumento analizza le immagini *in tempo reale* e le confronta con una banca dati preselezionata (cd. *watchlist*), contenente le informazioni biometriche di individui già segnalati o registrati in precedenza. Questa operazione avviene attraverso un meccanismo di estrazione dei *punti di repere*, che consente di identificare le caratteristiche distintive dei volti catturati e di metterle a confronto con le corrispondenze archiviate, restituendo un coefficiente di similarità che misura il grado di compatibilità tra i soggetti ripresi e quelli presenti nel database. Una volta acquisito un nuovo *frame*, il sistema avvia la ricerca, elaborando simultaneamente sia le immagini già memorizzate nel database, sia quelle estratte dallo *streaming* video *in tempo reale.* Tale modalità operativa permette di individuare in tempi estremamente ridotti eventuali corrispondenze biometriche, generando segnalazioni automatiche (*alert*) che necessitano tuttavia di una verifica successiva da parte degli operatori.

[85] Cfr. il § 4.3.

[86] Uno *stream* (anche detto "flusso") è un "canale" tra la sorgente e la destinazione attraverso il quale fluiscono i dati.

Le differenze tecniche che caratterizzano le due modalità di impiego di SARI risiedono principalmente nella tempistica del processo di comparazione biometrica rispetto alla fase di acquisizione del volto e nella dimensione della banca dati di riferimento su cui il sistema esegue l'analisi. Nella modalità *enterprise*, il confronto avviene con un ampio database di profili biometrici, acquisiti e archiviati precedentemente. Al contrario, la modalità *real-time* non effettua la ricerca su un archivio vasto e generalizzato, ma opera con una *watchlist* preselezionata dagli operatori, contenente esclusivamente i profili di alcuni soggetti. Dal punto di vista tecnico-operativo, questo approccio consente al sistema algoritmico di effettuare il confronto istantaneo tra i volti rilevati attraverso telecamere o altri dispositivi di acquisizione e quelli contenuti nella lista, senza dover effettuare l'analisi comparativa sull'intera banca dati. Questa modalità risponde a precise esigenze di efficienza computazionale, riducendo drasticamente la platea dei potenziali soggetti confrontabili e migliorando la velocità e l'accuratezza del confronto *in tempo reale.* Tale distinzione non si limita a rappresentare una mera differenza di natura tecnica, ma assume rilevanza anche sul piano giuridico, dando origine a diverse interpretazioni normative in merito all'inquadramento e alla disciplina applicabile ai sistemi di riconoscimento biometrico. In tale prospettiva, occorre sin da subito sottolineare come ogni componente tecnologica che concorre alla struttura funzionale di questi strumenti influisca direttamente sulla qualificazione giuridica degli stessi, condizionando non soltanto le modalità di trattamento dei dati personali, ma anche l'ampiezza e l'intensità delle garanzie approntate a tutela dei diritti fondamentali degli interessati [87].

4.2. *La banca dati AFIS – SSA*

In Italia, i principali archivi di dati biometrici a disposizione delle forze di polizia sono l'AFIS, *Automated Fingerprint Identification System* [88] e la banca dati nazionale del DNA, istituita con legge n. 85/2009 [89]. La prima è

[87] Cfr. il capitolo III.

[88] All'AFIS è agganciata l'APIS ("*automated palmprint identification system*"), banca dati di impronte palmari che viene utilizzata generalmente quando le impronte digitali risultano abrase o illeggibili.

[89] La normativa è stata completata successivamente con l'introduzione di un regolamento attuativo, il d.P.R. 7 aprile 2016, n. 87 contenente il regolamento recante disposizioni di

costituita da un database e da un sistema automatizzato di identificazione delle impronte digitali, integrato dal cd. "sottosistema anagrafico SSA", contenente le immagini segnaletiche e le relative informazioni anagrafiche e descrittive dei soggetti identificati [90]. L'impiego di AFIS si articola in due filoni applicativi, distinti per finalità e contesto operativo: da un lato, la ricerca decadattilare, o per rappresentazione digitalizzata dei volti a fini preventivi; dall'altro, l'analisi di frammenti papillari o del volto in ambito giudiziario. Nel primo caso, l'analisi consente di accertare la corrispondenza con entità già note al sistema e di ricostruire l'eventuale *iter* storico della loro inclusione in banche dati biometriche preesistenti [91]. Nel secondo caso, il ricorso ad AFIS assume una finalità investigativa o probatoria nel contesto di un procedimento penale avviato, configurandosi come una fase essenziale dell'*iter* di identificazione. La ricerca biometrica viene condotta per accertare l'identità della persona sottoposta a indagine, attraverso il confronto tra le tracce papillari o i dati biometrici utili alla ricostruzione del fatto e alla individuazione del colpevole e le informazioni archiviate nella banca dati.

Il "sottosistema anagrafico" (da qui, SSA) rappresenta l'applicativo attualmente impiegato dagli operatori di polizia scientifica per la gestione e la ricerca dell'identità di soggetti ignoti all'interno delle banche dati biometriche. Questo strumento costituisce un'estensione operativa del sistema AFIS,

---

attuazione della legge 30 giugno 2009, n. 85, concernente l'istituzione della banca dati nazionale del DNA e del laboratorio centrale per la banca dati nazionale del DNA, ai sensi dell'articolo 16 della legge n. 85 del 2009. Cfr. C. FANUELE, *Dati genetici e procedimento penale*, Cedam, Padova, 2009; L. MARAFIOTI-L. LUPARIA (a cura di), *Banca dati del Dna e accertamento penale*, Giuffrè, Milano, 2010; L. SCAFFARDI, *Giustizia genetica e tutela della persona. Uno studio comparato sull'uso (e abuso) delle Banche dati del DNA a fini giudiziari*, Wolters Kluwer Cedam, Milano, 2017.

[90] Le immagini presentano qualità e composizione eterogenea a seconda del tipo di dispositivo di acquisizione, del motivo del fotosegnalamento e del periodo storico in cui detta immagine è stata inserita nella banca dati. Potendo uno stesso soggetto essere stato fotosegnalato più volte, potrà verificarsi l'eventualità che differenti record siano legati da un unico Codice Univoco Identificativo (CUI).

[91] Una volta scansionato il cartellino segnaletico, esso viene inviato al Gabinetto di Polizia Scientifica ovvero al Reparto Dattiloscopia Preventiva dei Carabinieri. A questo punto, il dattiloscopista procede al controllo sulla qualità delle impronte eseguendo successivamente una ricerca nel database, il quale, in pochi minuti propone una serie di candidati compatibili. Il risultato negativo dell'accertamento implica che il soggetto sottoposto ai rilievi non sia stato fotosegnalato in precedenza, l'esito positivo, invece, mostra come lo stesso sia stato fotosegnalato altre volte, indicando contestualmente i dati d'interesse (per es. la data dei rilievi, il reparto segnalante e il motivo del fotosegnalamento).

con cui interagisce mediante un'infrastruttura software dedicata. Dal punto di vista tecnico, il SSA si configura come uno strumento di elaborazione avanzata, progettato per garantire un costante allineamento con i dati contenuti nell'AFIS. Il processo di sincronizzazione avviene attraverso un software *batch* [92], che consente il recupero sistematico dei nuovi inserimenti effettuati nella banca dati centrale. Questo meccanismo garantisce un aggiornamento continuo delle informazioni biometriche, assicurando che le operazioni di identificazione siano basate su un *dataset* sempre attuale e completo. L'interazione tra SSA e AFIS permette di ottimizzare le attività investigative, poiché consente un accesso rapido e strutturato alle informazioni archiviate. In particolare, il SSA facilita il confronto tra le impronte digitali o altre caratteristiche biometriche acquisite nel corso delle indagini e le corrispondenze già presenti nel sistema, fornendo così un supporto essenziale per le operazioni di riconoscimento.

L'intera banca dati trae alimentazione da fonti eterogenee, espressione di una pluralità di attività di rilevazione, che trovano il proprio fondamento giuridico in disposizioni normative di diversa natura. Il d.m. 24 maggio 2017, che regolamenta i trattamenti di dati personali effettuati dal Centro elaborazione dati rinvia, tra gli altri, agli artt. 4 TULPS, 349 c.p.p., al d.l. n. 59/1978 convertito con modificazioni dalla legge 18 maggio 1978, n. 191 e al d.lgs. n. 286/1998 [93]. Tali norme disciplinano una serie di attività di polizia

---

[92] Cfr. "*batch*", *Enciclopedie online*, Istituto dell'Enciclopedia italiana Treccani, http://www.treccani.it/enciclopedia/biometria/: in informatica, in contrapposizione a tempo reale e a *timesharing*, modalità di elaborazione secondo la quale le richieste di servizio non vengono assolte immediatamente, ma sono accodate per essere soddisfatte quando lo consentirà la disponibilità delle risorse.

[93] Individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, in attuazione dell'arti. 53, comma 3, d.lgs. 30 giugno 2003, n. 196. (17A04275), *G.U.*, Serie Generale n. 145 del 24 giugno 2017, Suppl. ord. n. 33. Così, la scheda tecnica n. 19 del Decreto del Ministero dell'Interno 24 maggio 2017, ha specificato come AFIS operativo presso il servizio di polizia scientifica della Direzione centrale Anticrimine della Polizia di Stato, gestisca il trattamento dei dati personali e identificativi acquisiti dai soggetti sottoposti a foto segnalamento a fini, tra gli altri, di: identificazione dattiloscopica di soggetti foto segnalati (art. 349 c.p.p.; art. 4 TULPS e art. 7 Regolamento di esecuzione; art. 5, d.lgs. n. 286/1998; legge n. 85/2009; regolamento UE n. 603/2013; Provvedimento generale prescrittivo in tema di biometria del Garante per la protezione dei dati personali n. 513/2014); esecuzione di accertamenti tecnici volti alla identificazione dei frammenti di impronta acquisiti

eterogenee, differenziandosi per finalità, presupposti applicativi e ambito di intervento.

Rispetto ad AFIS, la banca dati del DNA ha un contenuto molto più circoscritto e specifico. Infatti, al suo interno sono inseriti unicamente i profili dei soggetti di cui all'art. 9, commi 1 e 2 della legge 30 giugno 2009, n. 85 [94], i profili del DNA estratti dai reperti biologici acquisiti nel corso di procedimenti penali e relativi a persone scomparse o loro consanguinei, di cadaveri e resti cadaverici non identificati [95]. Da notare che il legislatore, allo scopo di garantire l'uniformità dei dati acquisiti, ha disciplinato anche la metodologia di analisi di reperti e campioni biologici per la tipizzazione dei profili genetici che confluiscono nella banca dati nazionale, individuando i parametri delle analisi in quelli riconosciuti a livello internazionale e indicati dall'*European Network of Forensic Sciences Institutes (*ENFSI) e sottoponendo l'inserimento nella banca dati alla condizione che i profili siano stati tipizzati in laboratori certificati a norma ISO/IEC [96].

---

sulla scena del crimine o sui reperti pertinenti al reato, in relazione a indagini condotte attraverso accertamenti tecnici effettuati dalle forze di polizia nell'ambito di un procedimento penale (Titolo IV e V c.p.p.; Provvedimento generale prescrittivo in tema di biometria del Garante per la protezione dei dati personali n. 513/2014); accertamenti per finalità investigativa mediante il sottosistema anagrafico (Titolo IV e V c.p.p.; art. 13 legge n. 124/2007; Provvedimento generale prescrittivo in tema di biometria del Garante per la protezione dei dati personali, n. 513/2014).

[94] Appartenenti a: a) soggetti ai quali sia applicata la misura della custodia cautelare in carcere o quella degli arresti domiciliari; b) i soggetti arrestati in flagranza di reato o sottoposti a fermo di indiziato di delitto; c) i soggetti detenuti o internati a seguito di sentenza irrevocabile, per un delitto non colposo; d) i soggetti nei confronti dei quali sia applicata una misura alternativa alla detenzione a seguito di sentenza irrevocabile, per un delitto non colposo; e) i soggetti ai quali sia applicata, in via provvisoria o definitiva, una misura di sicurezza detentiva.

[95] Inoltre, l'art. 9, comma 2 stabilisce che l'acquisizione dei campioni biologici possa avvenire solamente se si procede nei confronti di soggetti indagati, imputati o condannati per delitti non colposi per i quali è consentito almeno l'arresto in flagranza, e fornisce, in negativo, un elenco di reati per i quali non è possibile procedere a tale prelievo. P. FELICIONI, *L'acquisizione di materiale biologico a fini identificativi o di ricostruzione del fatto*, Cedam, Padova, 2009, p. 196 ss.

[96] L'*European Network of Forensic Science Institutes (*ENFSI), istituito nel 1995, rappresenta una rete europea di istituti di scienze forensi, il cui ambito di cooperazione si è progressivamente esteso, includendo, almeno per quanto concerne la genetica forense, anche l'FBI e istituzioni di paesi extraeuropei. L'ENFSI è stato concepito con l'obiettivo di facilitare lo scambio di informazioni nel settore delle scienze forensi, promuovendo la collaborazione tra laboratori e centri di ricerca, al fine di armonizzare metodologie di analisi e sviluppare standard operativi condivisi. Tra le sue principali attività rientrano la produzione di linee guida,

Vi sono certamente macroscopiche differenze tra il riconoscimento facciale e l'identificazione genetica, che potrebbero rendere il paragone fra le due banche dati assolutamente azzardato: basti pensare all'alta "distintività" delle caratteristiche genetiche, a differenza delle mere similarità presenti nei volti delle persone; l'immodificabilità della struttura del DNA di qualsiasi individuo nonostante il trascorrere del tempo, in contrapposizione all'"ipervariabilità" dei tratti somatici; la complessità delle operazioni laboratoriali legate all'analisi del materiale biologico e alla conservazione delle risultanze, rispetto ai processi algoritmici che regolano il confronto fra i volti; l'alta affidabilità dell'identificazione tramite il DNA, a fronte del tasso di errore insito nel riconoscimento facciale, specie se operato *in tempo reale;* la previsione di una metodologia di analisi dei reperti e dei campioni condivisa a livello internazionale, rispetto all'assenza di criteri di riferimento per l'inserimento delle immagini in AFIS.

La distinzione ontologica e funzionale tra le diverse categorie di dati biometrici si riflette inevitabilmente anche sulle relative procedure di acquisizione, trattamento e conservazione, determinando un'articolazione normativa e operativa differenziata. In tale prospettiva, le modalità previste per la raccolta e l'elaborazione dei dati biometrici destinati all'integrazione del sistema AFIS si distinguono in maniera sostanziale da quelle predisposte per la gestione della banca dati del DNA. Mentre la raccolta e la conservazione dei profili genetici avviene sulla base di presupposti normativi chiaramente definiti, con un impianto regolatorio che ne delimita l'uso esclusivo a fini giudiziari e per specifiche categorie di soggetti (come gli indagati per reati particolarmente gravi), le modalità di acquisizione e utilizzo dei dati biometrici in AFIS si caratterizzano per confini meno nitidi e criteri di inclusione più estesi.

La diversa natura delle operazioni che possono condurre all'inserimento di dati all'interno della banca dati AFIS evidenzia una mancanza di

---

la diffusione di raccomandazioni tecnico-scientifiche e la redazione di manuali metodologici, elementi fondamentali per garantire l'uniformità e l'affidabilità delle pratiche forensi nei diversi ordinamenti giuridici. Parallelamente, l'ENFSI svolge un ruolo cruciale nel guidare la comunità scientifica verso obiettivi comuni, promuovendo la ricerca applicata e lo sviluppo di nuove tecnologie forensi. In particolare, l'organizzazione è impegnata nell'ottimizzazione delle metodologie di analisi del DNA, attraverso l'elaborazione di progetti scientifici finalizzati a migliorare il potere informativo delle evidenze biologiche. In ambito nazionale, con l'obiettivo di favorire la condivisione delle conoscenze e di promuovere l'armonizzazione e l'adozione di metodiche analitiche standardizzate, la Polizia Scientifica prende parte attivamente ai lavori del Gruppo Ge.F.I. (Genetisti Forensi Italiani). Tale gruppo di lavoro, costituito nel 1975, opera all'interno della *International Society for Forensic Genetics* (ISFG) come sezione di riferimento per la comunità scientifica di lingua italiana.

armonizzazione sistematica, dal momento che l'acquisizione può derivare da contesti e finalità profondamente differenti. Come visto, se da un lato è prevista la registrazione di impronte digitali e immagini segnaletiche nell'ambito di attività di polizia giudiziaria connesse a un procedimento penale (ad esempio, nel caso di fotosegnalamento di soggetti arrestati o sottoposti a fermo), dall'altro, l'inserimento nella stessa banca dati può avvenire anche all'esito di semplici attività di prevenzione e controllo di pubblica sicurezza, senza che vi sia un'immediata correlazione con un'indagine in corso.

Sorge allora un interrogativo di primaria rilevanza: le differenze qualitative tra le diverse tipologie di dati biometrici sono tali da giustificare una disciplina normativa più o meno dettagliata in relazione ai metodi di raccolta e alimentazione delle rispettive banche dati? L'analisi della regolamentazione vigente suggerisce che l'estensione e la complessità della normativa sembrano essere direttamente proporzionali al grado di *acquisibilità* del dato biometrico. L'elevato contenuto informativo del dato genetico, unito alla complessità tecnico-scientifica delle operazioni necessarie alla sua estrazione e analisi, ha spinto il legislatore a introdurre un impianto normativo dettagliato, con limitazioni stringenti all'inserimento e all'utilizzo delle informazioni genetiche nei contesti investigativi e giudiziari. Al contrario, la relativa semplicità con cui è possibile acquisire un volto e la conseguente facilità di implementazione di sistemi di riconoscimento facciale sembrano aver favorito una disciplina meno restrittiva.

Si assiste, pertanto, ad un peculiare paradosso normativo: nonostante il volto presenti caratteristiche intrinseche che ne limitano l'affidabilità identificativa – quali la scarsa riferibilità individualizzante, l'elevata ipervariabilità in funzione di fattori ambientali e temporali, nonché la sua ridotta stabilità morfologica – esso risulta, sul piano giuridico, significativamente più accessibile e suscettibile di trattamento rispetto al dato genetico. Quest'ultimo, infatti, pur rappresentando un'informazione qualitativamente più stabile e univoca, è assoggettato a una disciplina normativa più rigorosa, che impone – per la sua acquisizione e tipizzazione – il rispetto di requisiti sostanziali e procedurali particolarmente stringenti, in ragione della valenza informazionale sensibile del profilo genetico e dei potenziali impatti sulla sfera intima e identitaria dell'individuo. Le implicazioni di tale disequilibrio non sono meramente teoriche, ma investono direttamente la sfera giuridica dell'individuo, incidendo, come si vedrà più avanti, su diritti costituzionalmente garantiti quali la riservatezza e la libertà di autodeterminazione [97].

[97] Cfr. il capitolo III.

4.3. *Tecniche di intelligenza artificiale e riconoscimento facciale*

Come visto, i tratti biometrici – tra cui il volto – si configurano quali entità multidimensionali, la cui analisi e trattamento richiedono lo studio di discipline eterogenee. Dalla biologia, su cui si basa la conformazione e la stabilità del tratto nel tempo, alla statistica, che ne quantifica l'unicità e la distribuzione nella popolazione, dalla fisica, che ne indaga le proprietà ottiche e la riflessione della luce, sino all'informatica, che elabora i modelli di rappresentazione digitale e i relativi algoritmi di comparazione: la tecnologia di riconoscimento facciale si pone all'intersezione di molteplici campi del sapere, ciascuno portatore di contributi indispensabili alla sua funzionalità e precisione. Tale interconnessione disciplinare costituisce il primo e più basilare «livello di complessità» [98] che permea il procedimento di riconoscimento facciale. Entro tale scenario, infatti, come sopra accennato, occorre tenere in considerazione l'impiego di tecniche di intelligenza artificiale (IA) [99] e degli

---

[98] L'espressione è di S. QUATTROCOLO, *Equità del processo penale e a*utomated evidence *alla luce della Convenzione europea dei diritti dell'uomo*, in *Revista Italo-Española de Derecho Procesal*, 2019, p. 2 ss.

[99] Da qui in avanti anche solo "IA". Questa espressione è stata utilizzata per la prima volta durante il convegno organizzato nel 1956 presso il Dartmouth College, in New Hampshire, avente ad oggetto lo sviluppo di macchine c.d. "intelligenti", ossia di macchine capaci di riprodurre il ragionamento umano e quindi la capacità di prendere decisioni attraverso l'apprendimento ed il ricorso a generalizzazioni. Il testo integrale del convegno è consultabile sul sito 250.dartmouth.edu. Sull'argomento cfr. il lavoro pioneristico di L. LUPARIA, *Prova giudiziaria e ragionamento artificiale: alcune possibili chiavi di lettura*, in J. SALLANTIN-J.J. SZCZECINIARZ (a cura di), *Il concetto di prova alla luce dell'intelligenza artificiale*, Giuffrè, Milano, 2005, p. 14 ss.; M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *Dir. pen. cont*., 2019, p. 1; G. CANZIO, *Intelligenza artificiale e processo penale*, in *Cass. pen.*, 3, 1 marzo 2021, p. 797; M. CAIANIELLO, *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 29, 2021, p. 1-23; J. NIEVA-FENOLL, *Intelligenza artificiale e processo* (trad. a cura di) P. Comoglio, Giappichelli, Torino, 2019, p. 7 ss.; M. TARUFFO, *Judicial decision and Artificial Intelligence*, in *Artificial Intelligence and Law*, 1998, p. 311 ss.; A. GARAPON-J. LASSÉGUE, *La giustizia digitale. Determinismo tecnologico e libertà*, il Mulino, Bologna, 2021, p. 143; S. QUATTROCOLO, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, 2020,p. 123; M. EBERS, *Regulating AI and Robotics: Ethical and Legal Challenges*, in M. EBERS-S.N. NAVARRO (a cura di), *Algorithms and Law*, Cambridge, University Press, Cambridge, 2019, p. 6 ss.; S. CONTISSA-G. LASAGNI-G. SARTOR, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Dir. Internet*, 4, 2019, p. 619 ss.

evidenti vantaggi offerti dalla diffusione dei cd. *big data* [100], enormi quantità di dati o immagini raccolte in ampi database e sfruttati al fine di ottimizzare i processi di riconoscimento.

Uno strumento di IA viene definito come un «sistema automatizzato progettato per funzionare con livelli di autonomia variabili, che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali» [101]. In altre parole, l'IA è «*the science of making machines do things that would require intelligence if done by man*» [102]. L'attitudine dell'essere umano a individuare schemi e instaurare correlazioni tra insiemi di dati trova oggi una declinazione tecnologica avanzata nei sistemi di intelligenza artificiale. Le architetture più evolute di tali strumenti non si limitano alla mera elaborazione automatizzata di ampi volumi di dati, né alla restituzione di risposte predefinite in base alla programmazione iniziale, ma sono in grado di sviluppare "capacità adattive", affinando progressivamente le proprie prestazioni mediante processi iterativi di apprendimento [103].

In tale contesto, i modelli consentono ai sistemi di estrapolare regolarità

---

[100] Cfr. T. TAULLI, *Artificial Intelligence Basics*, Apress, Berkeley, 2019, p. 23 ss.; G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 78; M.M. PLESNICAR-A. ZAVRŠNIK-P. ŠARF, *Fighiting Impunity with New Tools: How Big Data, Algorithms, Machine Learning and AI Shape the New Era of Criminal Justice*, in L. MARIN-S. MONTALDO (a cura di), *The Fight Against Impunity in EU Law*, Hart Publishing, New York, 2020; B. MITTELSTADT-L. FLORIDI, *The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts*, in *Science and Engineering Ethics*, 22, 2016.

[101] Cfr. l'art. 3, par. 1, n. 1 del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, 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), cfr. il capitolo IV, § 3.2. Per un approfondimento cfr. *ex multis* F. DONATI, *Intelligenza artificiale e giustizia*, cit., p. 415. Per un approfondimento sulle varie definizioni di IA cfr. G. ROMANO, *Diritto, robotica e teoria dei giochi: riflessioni su una sinergia*, in G. ALPA (a cura di), *Diritto e intelligenza artificiale*, Pacini, Pisa, 2020, p. 105; S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, cit., p. 7-8; C. PARODI-V. SELLAROLI, *Sistema penale e intelligenza artificiale: molte esperienze e qualche equivoco*, in*Dir. pen. cont.*, 6/2019, p. 64.

[102] Cfr. M. MINSKY, *Semantic Information Processing*, The MIT Press, Cambridge, 1968.

[103] Cfr. D. POLIDORO, *Tecnologie informatiche e procedimento penale: la giustizia penale messa alla prova dall'intelligenza artificiale*, in *Arch. pen.* (Web), 3, 2020, p. 4 e J. NIEVA-FENOLL, *Intelligenza artificiale e processo*, cit., p. 8.

statistiche dai dati in ingresso, migliorando la propria capacità predittiva e, nei *tool p*iù sofisticati, di giungere persino ad assumere decisioni in autonomia, sulla base di schemi inferenziali determinati dal cd. *training* effettuato sulla base dei dati di riferimento (*dataset*) [104]. A tal proposito, si è soliti distinguere fra l'apprendimento automatico, o cd. *machine learning* [105], ossia meccanismi in grado di "imparare" il mondo esterno e, stabilendo delle correlazioni, trarre delle conclusioni o prendere delle decisioni [106], e l'IA in grado di estrarre sistemi complessi di valutazione sulla base di grandi volumi di dati immessi dall'uomo [107].

Il *machine learning* ha trovato ampio sviluppo anche grazie al supporto offerto dalle cd. reti neurali artificiali [108], ossia meccanismi di elaborazione delle informazioni ispirati al funzionamento del sistema nervoso proprio delle reti neurali e del cervello umano [109]. Tale tecnologia è in grado di acquisire la capacità di imparare i cd. *patterns* (o "schemi") e le associazioni

---

[104] L'"algoritmo" può essere definito come un'istruzione matematica (o "codice") impiegata al fine di risolvere un problema, dare una risposta ad un quesito ovvero svolgere determinate funzioni. Cfr. T. GILLESPIE, *The relevance of algorithms*, in T. GILLESPIE-P. BOCZKOWSKI-K. FOOT (eds.), *Media technologies*, The MIT Press, Cambridge, 2014, p. 167.

[105] L'espressione *machine learning* si riferisce a sistemi che riescono ad estrarre automaticamente modelli significativi da grandi quantità di dati. Cfr. al riguardo S. SHALEV SHWARTZ-S. BEN DAVID, *Understanding Ma-chine Learning: From Theory to Algorithms*, Cambridge University Press, New York, 2014.

[106] Cfr. M. EBERS, *Regulating AI and Robotics: Ethical and Legal Challenges*, in M. EBERS-S.N. NAVARRO (a cura di), *Algorithms and Law*, Cambridge University Press, Cambridge, 2019, p. 7.

[107] Cfr. R. LOPEZ, *Riconoscimento facciale tramite software e individuazione del sospettato*, in A. SCALFATI (a cura di), *Pre-Investigazioni*, Giappichelli, Torino, 2020, p. 296; F. MAGGINO-G. CICERCHIA, *Algoritmi, etica e diritto*, cit., p. 1161; T. TAULLI, *Artificial Intelligence Basics*, Apress, Berkeley, 2019, p. 4.

[108] Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 54. Sull'impiego delle reti neurali nei software di riconoscimento facciale v. S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, 2020, p. 65-66; V. MANFREDI-E. PESSA, *Il riconoscimento dei volti: aspetti cognitive, neuropsicologici e computazionali*, in *Sist. intell.*, 3, 2011, p. 447 ss.; G. VESSIO, *Intelligenza artificiale per curiosi. Una mini-guida scientifica per tutti*, Dedalo, Bari, 2025.

[109] Cfr. sul punto G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 54. Sull'impiego delle reti neurali nei software di riconoscimento facciale v. S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, cit., p. 65-66 e V. MANFREDI-E. PESSA, *Il riconoscimento dei volti: aspetti cognitive, neuropsicologici e computazionali*, cit., p. 447 ss.

esistenti fra essi, senza essere state programmate per eseguire tale operazione e apprendendo autonomamente dalla propria esperienza [110].

A partire dagli anni Settanta del secolo scorso – e a cavallo delle alterne stagioni che hanno segnato la breve ma pur intensa storia dell'IA, caratterizzata dal passaggio dall'approccio logico-matematico a quello puramente statistico – il settore della *computer vision* ha registrato un significativo avanzamento, determinando una rapida evoluzione degli algoritmi di estrazione e analisi delle informazioni visive. Questo sviluppo ha favorito la nascita di un filone di ricerca altamente specializzato nell'ambito del riconoscimento facciale, consentendo l'elaborazione di modelli computazionali sempre più precisi e adattabili alle esigenze operative nei diversi contesti applicativi [111]. L'estrazione automatizzata delle caratteristiche di *input p*er la generazione dei risultati di *output* si basa oggi su livelli progressivi di astrazione e classificazione, attraverso cui il sistema è in grado di identificare schemi ricorrenti (*patterns*) all'interno di dati non strutturati. In particolare, il processo di riconoscimento può partire dall'analisi dei *pixel* di un'immagine digitale, passando per la rilevazione dei contorni e delle forme, fino a giungere a una rappresentazione più complessa dell'oggetto analizzato [112].

Un aspetto di fondamentale rilevanza, anche in questo settore, è rappresentato dal mutamento di paradigma che ha contraddistinto la ricordata evoluzione dall'approccio logico a quello statistico. Mentre in passato il riconoscimento facciale si basava su regole predeterminate codificate dallo sviluppatore, oggi il software stesso è in grado di instaurare autonomamente criteri di correlazione e corrispondenza, esaminando le immagini contenute nel *dataset s*u cui è stato addestrato. Tale transizione è stata resa possibile dall'implementazione di tecniche avanzate di apprendimento automatico, le quali permettono agli algoritmi di individuare schemi ricorrenti e di formulare correlazioni predittive, anche in assenza di un impulso umano [113].

---

[110] Cfr. V. MANFREDI-E. PESSA, *Il riconoscimento dei volti: aspetti cognitivi, neuropsicologici e computazionali*, cit., p. 456.

[111] «*A series of steps undertaken in order to solve a particular problem or accomplish a defined outcome*». R. KITCHIN, *Thinking critically about and researching algorithms*, in *Information, Communication and Society*, 20(1), 2017, p. 1-14; K.A. GATES, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*, New York University Press, New York, 2011, p. 31.

[112] Cfr. P. KAUR-K. KRISHAN-S.K. SHARMA-T. KANCHAN, *Facial-recognition algorithms: a literature review*, cit., p. 136.

[113] Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 53. Un grande impulso nello studio dell'IA è stato dato con il passaggio dal ragionamento basato sulle regole (RBR)

Inoltre, un ulteriore e decisivo progresso tecnologico si è compiuto con l'introduzione e la progressiva implementazione delle tecniche di *deep learning*, le quali hanno radicalmente modificato le modalità di elaborazione e analisi delle immagini biometriche, in particolare di quelle facciali [114]. Le reti neurali profonde (*deep neural networks*), basate su architetture multilivello, consentono oggi di eseguire operazioni di scomposizione, astrazione e classificazione dei dati visivi secondo una struttura gerarchica, in cui ogni livello successivo elabora le informazioni in modo sempre più sofisticato rispetto al precedente. Questa modalità permette al sistema di estrarre in modo autonomo le caratteristiche salienti (*features*) del volto, riducendo la necessità di intervento umano nella fase di programmazione iniziale e conferendo al sistema una capacità adattiva che si perfeziona attraverso l'addestramento su grandi moli di dati. La capacità discriminativa di tali reti consente non solo di identificare la mera presenza di un tratto biometrico, ma di effettuare analisi comparative ad alta precisione, individuando analoghe ricorrenze o differenze sottili tra soggetti distinti, anche in condizioni ambientali complesse o variabili [115].

---

al ragionamento basato sui casi (CBR, *dal termine inglese Case-based reasoning*). Il ragionamento basato sui casi, teorizzato da Roger Schank nei primi anni Ottanta del XX secolo, "*is a problem solving paradigm where new problems (called target or query problems) are solved by retrieving similar problems already solved, possibly by adapting the solutions of such retrieved problems*". Trattasi di un processo di risoluzione di nuovi problemi basato sulle soluzioni di problemi precedenti. Per un approfondimento sul tema vedi S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, cit., p. 111 ss.

[114] Cfr. *ex multis* N. CAULI-A. ORTIS-S. BATTIATO, *Fooling a Face Recognition System with a Marker-Free Label-Consistent Backdoor Attack*, in *Image Analysis and Processing-ICIAP 2022: 21st International Conference*, Lecce, Italy, May 23-27, 2022, Proceedings, Part II, p. 176-185; Q. CAO-L. SHEN-W. XIE-O.M. PARKHI-A. ZISSERMAN, *VGGFace2: a dataset for recognising faces across pose and age, in International Conference on Automatic Face and Gesture Recognition*, 2018; O.M. PARKHI-A. VEDALDI-A. ZISSERMAN, *Deep face recognition*, in *Proceedings of the British Machine Vision Conference (BMVC)*, p. 41.1-41.12, 2015; Y. TAIGMAN-M. YANG-M. RANZATO-L. WOLF, *DeepFace: closing the gap to human-level performance in face verification*, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2014, p. 1701-1708.

[115] Cfr. G. VESSIO, *Intelligenza artificiale per curiosi. Una mini-guida scientifica per tutti*, Dedalo, Bari, 2025; C. AITKEN-F. TARONI, *Statistics and the Evaluation of Evidence for Forensic Scientists*, Wiley, New York, 2004; C. AITKEN-R. ROBERTS-G. JACKSON, *Fundamentals of probability and statistical evidence in criminal proceedings: guidance for judges, lawyers, forensic scientists and expert witnesses*, Royal Statistical Society, London, 2010; D.H. KAYE, *Statistics for lawyers and law for statistics*, in 89 *Mich. L. Rev.*, 1991, p. 1520.

Il risultato di questa rivoluzione tecnologica è una significativa riduzione del margine di errore, in termini sia di falsi positivi sia di falsi negativi, che ha contribuito a rafforzare l'affidabilità dei sistemi di riconoscimento facciale in contesti applicativi sempre più eterogenei. Tuttavia, fa da contraltare la complessità dei modelli interni alle reti neurali profonde – spesso non pienamente intelligibili neppure agli sviluppatori (cd. *black box effect*) – che ha sollevato diverse questioni in ordine alla trasparenza, alla verificabilità e alla riproducibilità dell'*output* algoritmico [116]. Gli effetti derivanti dall'impiego di tali tecnologie saranno oggetto di un'analisi più approfondita nei successivi paragrafi, dove se ne esamineranno in dettaglio le implicazioni giuridiche e i riflessi sul piano delle garanzie fondamentali [117], alla luce del complesso bilanciamento tra efficienza operativa e tutela dei diritti dell'individuo.

4.4. *Il calcolo del rapporto di verosimiglianza nella scienza forense*

Si è detto che i sistemi di riconoscimento biometrico automatizzati sono in grado di effettuare il confronto tra due immagini digitalizzate, restituendo un punteggio numerico che rappresenta il grado di similarità tra i dati analizzati. Allo stato attuale, infatti, la tecnologia non consente, per tutti i dati biometrici sottoposti a confronto, la determinazione in via automatizzata della *tipicità* del campione, ossia la capacità di stabilire in termini statistici quanto una determinata caratteristica biometrica sia diffusa all'interno di una *popolazione di riferimento* [118]. Con tale espressione si intende un insieme statisticamente significativo di individui, i cui tratti biometrici sono stati oggetto di raccolta, analisi e catalogazione, così da costituire un parametro comparativo per valutare la *tipicità* o *rarità* di un determinato campione biometrico.

---

[116] Si rimanda al capitolo III, § 5.

[117] Cfr. il capitolo III.

[118] Tale principio non trova applicazione nel caso delle tecnologie di riconoscimento automatico o semi-automatico del parlatore, né per i software di comparazione del Dna in ragione dell'elevato grado di affidabilità scientifica raggiunto da tali strumenti, resi ormai capaci – grazie all'evoluzione dei modelli computazionali – di calcolare autonomamente la *tipicità* del dato e di stimare la probabilità relativa che un determinato tratto (vocale o genetico) provenga da un soggetto specifico rispetto a un membro qualsiasi di una popolazione di riferimento statisticamente definita.

L'impossibilità tecnica per il sistema di quantificare la distribuzione statistica di un tratto rende il processo di riconoscimento squisitamente probabilistico, impedendo che l'*output* del sistema possa essere considerato un indicatore assoluto dell'identità di un soggetto. Il risultato prodotto si configura, infatti, come un indice di similarità tra il dato analizzato e quelli presenti nel database di riferimento [119]. La mera somiglianza morfologica o corrispondenza formale, in assenza di un ancoraggio statistico, non garantisce da sola una qualificazione probatoria robusta e giuridicamente sostenibile, rischiando di generare falsi positivi o errori di identificazione, soprattutto in contesti eterogenei per distribuzione demografica, etnica o fenotipica.

Affinché questa percentuale di compatibilità assuma significato e possa essere considerata più affidabile e precisa nell'*iter* di riconoscimento e identificazione, occorre eseguire in via analogica il calcolo del "rapporto di verosimiglianza" (*likelihood ratio*, LR) [120]. Tale parametro, ottenuto attraverso metodologie statistiche differenti, rappresenta il rapporto tra due elementi fondamentali: il grado di similarità tra i campioni a confronto, ossia la compatibilità del dato ignoto rispetto a quello noto (numeratore), e la tipicità del campione analizzato, ovvero la sua diffusione all'interno di una specifica popolazione di riferimento (denominatore) [121]. Esso rappresenta un indicatore

---

[119] Cfr. K. NANDAKUMAR-Y. CHEN-S.C. DASS-A. JAIN, *Likelihood Ratio-Based Biometric Score Fusion*, in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 30(2), p. 342-347, 2008; M. EL-ABED-C. CHARRIER-C. ROSENBERGER, *Evaluation of biometric systems*, in *New Trends and Developments in Biometrics*, 2012, p. 149-169.

[120] Cfr. G. TESSITORE, *Riconoscimento automatico del volto e confronto in ambito forense*, in P. DI SIMONE-A, MANGIARACINA-L. PARLATO (a cura di), *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, Palermo University Press, Palermo, 2023, p. 80 ss.; *Best Practice Manual for Facial Image Comparison*, pubblicate dall'ENFSI-BPM-DI-01 Version, 01 – January 2018, reperibili su https://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf; T. BOVE-P. E. GIUA-A. FORTE-C. ROSSI, *Un metodo statistico per il riconoscimento del parlatore basato sull'analisi delle formanti*, in *Statistica*, anno LXII, n. 3, 2002, p. 480; C. AITKEN-F. TARONI, *Statistics and the Evaluation of Evidence for Forensic Scientists*, Wiley, New York, 2004; C. AITKEN-R. ROBERTS-G. JACKSON, *Fundamentals of probability and statistical evidence in criminal proceedings: guidance for judges, lawyers, forensic scientists and expert witnesses*, Royal Statistical Society, London, 2010; D.H. KAYE, *Statistics for lawyers and law for statistics*, in 89 *Mich. L. Rev.*, 1991, p. 1520.

[121] Cfr. G. TESSITORE, *Riconoscimento automatico del volto e confronto in ambito forense*, in P. DI SIMONE-A. MANGIARACINA-L. PARLATO (a cura di), *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, cit., p. 81; A.M. RODRIGUEZ-Z. GERADTS-M. WORRING, *Likelihood Ratios for Deep Neural Networks in Face Comparison*, in *JFS*, 2020, p. 5 ss.

quantitativo fondamentale nella valutazione del confronto biometrico, poiché consente di esprimere in termini probabilistici il grado di supporto che l'elemento raccolto fornisce a una determinata ipotesi identificativa.

L'integrazione del rapporto di verosimiglianza nel calcolo della compatibilità biometrica assume un ruolo cruciale, poiché permette di superare i limiti di un mero confronto tra i tratti facciali, introducendo un modello di valutazione basato su probabilità condizionate. Questo approccio, ampiamente consolidato nella metodologia forense, consente di ridurre il rischio di falsi positivi e falsi negativi, migliorando l'accuratezza delle decisioni basate sull'*output* del sistema automatizzato.

Nei capitoli successivi, si analizzerà il ruolo determinante del calcolo della verosimiglianza nel contesto procedimentale, entro cui i volti e, più utilmente, i *matches* possono essere acquisiti ed elaborati nell'ambito delle indagini [122]. Per il momento è sufficiente sottolineare l'imprescindibile necessità di un parametro statistico affidabile che supporti l'interpretazione del risultato biometrico, garantendone la completezza di calcolo. La successiva indagine si concentrerà sugli effetti processuali derivati, evidenziando come la mancanza di un criterio di valutazione probabilistica possa compromettere non solo l'attendibilità tecnica del riconoscimento, ma anche la sua capacità dimostrativa rispetto ai fatti oggetto di prova.

4.5. *Le finalità di verifica, identificazione e categorizzazione biometrica*

Un'ulteriore necessaria distinzione tecnica concerne le finalità applicative di categorizzazione, di identificazione e di verifica dell'identità [123]. Rispetto a quest'ultima, «il confronto di un campione biometrico presentato con il corrispondente dato biometrico registrato, relativo ad una singola

---

[122] Cfr. il capitolo V, § 6.1.1.

[123] Cfr. G. IOVANE, *Metodi matematici e tecnologie informatiche per l'analisi delle immagini in biometria e sicurezza*, Aracne, Roma, 2008, p. 171 ss.; A. JAIN-R. BOLLE-S. PANKANTI, *Biometrics. Personal identification in Networked Society*, Springer Science, New York, 1999, p. 2 ss.; W.S. COATS-A. BAGDASARIAN-T.J. HELOU-T. LAM, *The practitioner's Guide to Biometrics*, American Bar Association, Chicago, 2007, p. 5-6; J.L. WAYMAN, *Biometric Verification/Identification/Authentication/Recognition: The Terminology*, in A.K. JAIN-ARUN ROSS-S. PRABHAKAR (a cura di), *Encyclopedia of Biometrics, An Introduction to Biometric Recognition*, in *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 2004; C. GIUSTOZZI, *Giuristi e informatici divisi da una lingua comune: autenticazione?*, in http://www.interlex.it/forum10/relazioni/24giustozzi.htm.

persona» [124], viene eseguito al fine di accertare che l'individuo sia realmente chi dichiara di essere [125]. In altre parole, i sistemi biometrici di autenticazione/verifica accertano la compatibilità fra due dati, effettuando un raffronto di tipo "*one to one*" (1:1) fra determinate caratteristiche fisiche o comportamentali – già trasformate in *template* o semplicemente convertite in immagini digitali – e un *set* di valori precedentemente fornito dallo stesso utente e registrato in un database o in un dispositivo mobile [126].

I dati biometrici sono elaborati matematicamente e registrati all'interno della memoria di una base di dati centralizzata, al fine di poter eseguire il cd. *match* con l'identità richiesta [127]. Il soggetto può possedere altresì una *smart*

---

[124] Cfr. COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, p. 8: «*Verification means comparing a presented biometric sample with the corresponding enrolled biometric data pertaining to one single person*».

[125] Cfr. S. AMATO-F. CRISTOFARI-S. RACITI, *Biometria. I codici a barre del corpo*, cit., p. 135 e J.L. WAYMAN, *Fundamentals of biometric authentication technology*, in *Proceedings CardTech/Securtech*, Chicago, 1999.

[126] «Rientra in questa categoria la verifica dell'identità di un soggetto in possesso di uno *smartphone* mediante l'uso del lettore di impronta digitale, inserito nel dispositivo elettronico. Un software dedicato stabilisce infatti la corrispondenza tra l'impronta raccolta al momento della verifica (quando cioè l'utilizzatore vuole accedere al proprio *device*) e quella memorizzata e conservata nel dispositivo stesso sin dalla sua configurazione. Ancora è il caso delle carte d'identità elettroniche, munite di *chip*, all'interno del quale è contenuta una copia delle impronte digitali raccolte al momento della erogazione del documento; nel caso in cui si volesse verificare l'identità del possessore del documento, verrà effettuato un *match* tra il dato biometrico fornito al momento del controllo e quello immagazzinato nel *chip* del documento. Ben si comprende come il confronto sia uno-a-uno: il dato 'sorgente', da confrontare con quello di volta in volta fornito, è infatti solo uno». G. FORMICI, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, in *Saggi – DPCE online*, 2, 2019, p. 1111; EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, par. 10; S. BISI, *Il furto d'identità: panoramica attuale e prospettive giuridiche*, cit., p. 314; G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., p. 120. L'ISO/IEC 2382-37:2022 distingue l'autenticazione intesa come «*act of proving or showing ti be undistputed origin or veracity*» dalla verifica definita come «*process of confirming a biometric claim (…) through comparison*».

[127] «*Biometric verification is the comparison of a biometric sample offered at the point of transaction to a biometric template that is linked to a token (usually a PIN or access card) that the individual also presents at the point of transaction (a one-to one comparison). The use of a token in verification systems decreases processing time because a verification system compares the biometric that is presented only to the biometric template that is associated with the presented token. An identification system's flexibility with a verification system's reduced*

card, ovvero un *chip* integrato in un documento d'identità, in cui sia archiviato e conservato un suo dato biometrico, tramite il quale, davanti al dispositivo di cattura può essere effettuato un confronto tra il dato rilevato e quello registrato nel supporto [128].

Diversamente, l'"identificazione" consiste in un procedimento di attribuzione dell'identità che si realizza attraverso il raffronto dei dati biometrici di un soggetto ignoto con tutti quelli registrati in un archivio centralizzato [129], eseguendo così un confronto "*one to many*" (1:N, 1:N+1) [130]. L'identificazione si realizza qualora il sistema determini, all'interno di una fascia di tolleranza prefissata, un *template* biometrico che presenti il più alto grado di similarità con il campione acquisito. Anche nel caso in cui il soggetto non sia presente all'interno dell'archivio biometrico, l'operazione di confronto risulta comunque significativa, poiché permette di escludere che l'individuo appartenga al *dataset* considerato [131].

Infine, la categorizzazione consiste in un processo avanzato di estrazione e classificazione delle informazioni biometriche, finalizzato all'analisi e all'elaborazione di modelli statistici di distribuzione e frequenza. Tale metodologia consente di individuare *patterns* ricorrenti all'interno di un *dataset*, fornendo strumenti per la modellizzazione e lo studio delle caratteristiche biometriche in ambiti multidisciplinari [132]. La categorizzazione biometrica si distingue dall'identificazione e dalla verifica dell'identità, poiché non mira a riconoscere un individuo, bensì a raggruppare soggetti, favorendo la creazione di classi basate su caratteristiche statistiche comuni.

---

transaction time». W.S. COATS-A. BAGDASARIAN-T.J. HELOU-T. LAM, *The practitioner's Guide to Biometrics*, cit., p. 6.

[128] Cfr. S. AMATO-F. CRISTOFARI-S. RACITI, *Biometria. I codici a barre del corpo*, cit., p. 135.

[129] Ne consegue che, al fine di compiere confronti aventi scopo di identificazione, le banche dati a disposizione devono contenere ingenti quantità di dati. Talvolta, le rappresentazioni digitalizzate sono confrontate con quelle archiviate nei database in cui è nota la presenza del dato del soggetto interessato (*closed-set identification*, 1:N); altre volte non si è a conoscenza della presenza del dato del soggetto all'interno del database (*open-set identification*, 1:N+1).

[130] Cfr. W.S. COATS-A. BAGDASARIAN-T.J. HELOU-T. LAM, *The practitioner's Guide to Biometrics*, cit., p. 6. Per una panoramica generale sulla distinzione fra autenticazione e identificazione si veda S. AMATO-F. CRISTOFARI-S. RACITI, *Biometria. I codici a barre del corpo*, cit., p. 134 e *Linee-guida in materia di riconoscimento biometrico e firma grafometrica; Allegato A al Provvedimento del garante del 12 novembre 2014.*

[131] Cfr. S. AMATO-F. CRISTOFARI-S. RACITI, *Biometria. I codici a barre del corpo*, cit., p. 135.

[132] Cfr. K. MATHER, *Elementi di biometria*, Boringhieri, Torino, 1972, p. 25.

4.5.1. *Il riconoscimento delle emozioni*

Una peculiare applicazione dei sistemi di riconoscimento facciale impiegati per finalità di "categorizzazione" è quella che, a partire da una rappresentazione digitalizzata di un volto, permette di decifrare e associare le emozioni di un soggetto (cd. "*affective computing*" o "*sentiment analysis*")[133]. Sebbene questa specifica modalità applicativa non sia oggetto del presente studio, l'idea di schematizzare e riassumere l'individuo in categorie prestabilite, che ne è alla base, costituisce un elemento trasversale nell'ambito dell'intera trattazione e tornerà nei prossimi paragrafi come uno dei principali limiti di questa tecnologia.

In particolare, gli ambiti di applicazione interessati attengono alla realizzazione di sistemi capaci di riconoscere le emozioni dell'utente (riconoscimento emotivo), influenzarne lo stato emotivo (manipolazione emotiva), riprodurre (espressione emotiva) o provare stati d'animo (sintesi emotiva). La tecnologia si basa sull'analisi di determinati punti di riferimento (come gli occhi, le sopracciglia, il naso e la bocca) e gli adiacenti punti di contrazione dei muscoli[134]. L'*affective computing* implica non solo che il rapporto fra le manifestazioni esteriori e lo stato d'animo interiore siano perfettamente coincidenti, ma anche che le tecnologie di riconoscimento facciale siano in grado di cogliere le molteplici microespressioni del volto e di ricostruire lo stato psicologico-emotivo del soggetto[135]. Com'è stato osservato, tale tecnologia ha il limite di escludere completamente dalla valutazione fattori come la comunicazione interattiva, la connessione empatica, la capacità interpretativa dei sentimenti a partire dal sentire comune o dalla sensibilità culturale e l'analisi del contesto[136].

---

[133] Per un approfondimento cfr. E.H. HOUSSEIN-A. HAMMAD-A.A. ALI, *Human emotion recognition from EEG-based brain-computer interface using machine learning: a comprehensive review*, in *Neural Comput & Applic*, 34, 2022, p. 12527-12557; R.W. PICARD, *Affective Computing*, The MIT Press, Cambridge, 2000, p. 165; A. MCSTAY, *Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy*, in *Big Data & Society*, 2020, p. 1; I. NERONI REZENDE, *Can we use AI and neuroscience to detect lies in criminal proceedings? A European perspective*, in www.limablog.org, 2024.

[134] Cfr. J.M. HARLEY, *Measuring Emotions: A Survey of Cutting Edge Methodologies Used in Computer-Based Learning Environment Research*, in S.Y. TETTEGAH-M. GARTMEIER (eds.), *Emotions, Technology, Design, and Learning*, Elsevier Academic Press, Cambridge, 2016, p. 89 ss.

[135] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, p. 43.

[136] G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 43.

Il funzionamento di queste tecniche si basa su alcuni studi condotti, a partire dagli anni '60, dallo psicologo Paul Ekman, il quale sosteneva che tutte le emozioni possono essere ricondotte in sei macro categorie indipendentemente dal contesto socioculturale di provenienza: rabbia, disgusto, paura, felicità, tristezza e sorpresa [137].

Diversi studi successivi hanno ampiamente dimostrato che, in realtà, il modo con cui le persone manifestano le proprie emozioni varia considerevolmente tra culture, ambienti e persino tra singole persone in circostanze simili [138]. In una prospettiva antropologica e sociolinguistica, le espressioni facciali e le manifestazioni emotive non possono essere considerate indicatori universali e oggettivi, ma sono soggette a convenzioni sociali e norme culturali che influenzano il modo in cui le emozioni vengono percepite e interpretate [139].

Anche in ambito neuroscientifico e psicofisiologico, le evidenze empiriche mostrano che la correlazione tra stati emotivi interni e manifestazioni esteriori non è lineare né deterministica. Ad esempio, reazioni fisiologiche come la dilatazione della pupilla, l'aumento della sudorazione o le variazioni nel tono muscolare facciale possono essere influenzate da fattori situazionali, stress, esperienze pregresse e stati cognitivi concorrenti, rendendo difficile una decodifica oggettiva e univoca delle emozioni attraverso strumenti automatizzati. Nonostante ciò, tali tecniche hanno trovato applicazione negli ambiti più disparati: in campo medico sono state sfruttate per fornire assistenza sanitaria personalizzata a soggetti particolarmente vulnerabili [140];

---

[137] Cfr. P. EKMAN, *Basic emotions*, in T. DALGLEISH-M. POWER (a cura di), *Handbook of Cognition and Emotion*, 1999 e V.P. EKMAN, *Universality of Emotional Expression? A Personal History of the Dispute*, in P. EKMAN (ed.), *The Expression of the Emotions in Man and Animals*, III ed., Oxford University Press, New York, 1998, p. 363-393.

[138] Cfr. R. LEYS, *How Did Fear Become a Scientific Object and What Kind of Object Is It?*, Representations 110, no. 1 (2010), p. 66-104; L.F. BARRET *et al.*, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, in *Psychological Science in the Public Interest*, 20(1), 2019, p. 1-68.

[139] Cfr. H. HWANG-D. MATSUMOTO, *Evidence for the universality of facial expressions of emotion*, in M.K. MANDAL-A. AWASTHI (eds.), *Understanding facial expressions in communication: Cross-cultural and multidisciplinary perspectives*, 2015, p. 41-56; S.S. TOMKINS, *Affect, imagery, consciousness*, Vol. 1. *The positive affects*, Springer, New York, 1962; K.R. SCHERER-H.G. WALLBOTT, *Evidence for universality and cultural variation of differential emotion response patterning*, in *Journal of personality and social psychology*, 66(2), 1994, p. 310 ss.

[140] Cfr. B. SUBRAMANIAN-J. KIM-M. MARAY-A. PAUL, *Digital Twin Model: A Real-Time Emotion Recognition System for Personalized Healthcare*, in *IEEE*, 10, 2022, p. 81155-81165.

oppure, in ambito commerciale, tale tecnologia è stata impiegata per rilevare le preferenze e le risposte da parte dei consumatori [141]. Si tratta di impieghi ancora in via di sperimentazione che basano il loro funzionamento su calcoli computazionali aventi la "pretesa" di rintracciare e riconoscere determinati schemi, etichettandoli come "stati d'animo" o "emozioni".

4.6. *Livello di accuratezza e tipologie di errore nella tecnologia di riconoscimento facciale*

Generalmente, le misurazioni biometriche del volto, su cui si fonda il processo di riconoscimento facciale, presentano un elevato grado di variabilità, determinato da una combinazione di fattori intrinseci ed estrinseci che possono influenzare l'accuratezza e l'affidabilità del sistema [142]. Tali variabili incidono significativamente sulla qualità del dato biometrico, rendendo altamente improbabile che due campioni della medesima caratteristica, acquisiti in momenti diversi, risultino perfettamente identici [143].

Come già anticipato, l'eterogeneità delle condizioni di acquisizione può essere determinata da molteplici elementi, tra cui la presenza di un rumore digitale, le variazioni di illuminazione, le modificazioni della fisionomia del soggetto o un'interazione non ottimale con l'interfaccia del sistema. Assume un ruolo rilevante l'ambiente in cui il dato viene acquisito che può essere un contesto "controllato", come per esempio un ufficio di polizia o di frontiera, oppure un contesto in cui le condizioni di luce, distanza e posizionamento dell'individuo non sono controllate. Questi fattori, oltre a influenzare l'accuratezza della misurazione, incidono anche sulla percentuale di errore del sistema; aspetto che costituisce uno dei temi più complessi e articolati nell'intero ambito dell'analisi biometrica forense [144].

---

[141] AI NOW INSTITUTE, *AI Now Report 2019*, p. 50 ss., S. MONTEITH-T. GLENN-J. GEDDES *et al.*, *Commercial Use of Emotion Artificial Intelligence (AI): Implications for Psychiatry*, in *Curr. Psychiatry Rep*, 24, 2022, p. 203-211.

[142] Cfr. V.L. RAPOSO, *When facial recognition does not 'recognise': erroneous identifications and resulting liabilities*, in *AI & Soc*, 2023.

[143] Il successo di un sistema di riconoscimento dipende in gran parte dalla qualità dei campioni registrati nella banca dati (fattori endogeni o esogeni possono influire sulla corretta acquisizione del campione: per esempio nel caso del sudore di un polpastrello o della voce alterata dal raffreddore).

[144] Cfr. M. MENDOLA, *Aspetti informatici delle prove biometriche. Il problema dei "Falsi positivi"*, in *Psicol. e giust.*, anno 14, n. 1, 2013.

L'affidabilità dei sistemi di riconoscimento può risultare condizionata anche dalle specifiche caratteristiche somatiche delle persone da identificare. Infatti, tra i diversi dati, il volto risulta caratterizzato da un grado di "riferibilità individualizzante" più basso rispetto ad altri tratti [145]. È già stato segnalato, infatti, che *features* biometriche come il DNA, le impronte digitali e l'iride, avendo ad oggetto un'informazione biologica o biochimica strutturale permanente, presentano un più alto grado di "tipicità" o "distintività". Differenze marcate o, al contrario, somiglianze troppo accentuate, come nel caso dei gemelli, possono "ostacolare" la tecnologia, traendola in inganno durante una comparazione automatizzata [146].

A ciò si aggiungano le specificità delle immagini contenute nei database di riferimento, così come quelle impiegate durante la fase di sviluppo degli algoritmi, aspetti che possono ulteriormente incidere sulle prestazioni del sistema. A questo proposito, occorre considerare anche le possibili "distorsioni" (cd. *bias*) che possono verificarsi durante il procedimento di riconoscimento. Nella letteratura informatica, con il termine "*bias*" si indicano le distorsioni presenti all'interno di sistemi informatici che hanno l'effetto, tra l'altro, di escludere, includere e discriminare ingiustamente e sistematicamente determinati individui o gruppi in favore di altri. Questi fenomeni possono avere diverse origini e integrare una casistica molto varia: i *bias* possono avere origine già nella prima fase di costruzione del modello algoritmico, producendo "discriminazioni dirette", nella misura in cui siano impiegate delle "etichette" (cd. "*labels*") come "razza", "etnia", "genere", per categorizzare i dati e consentire agli algoritmi di distinguerli ai fini delle decisioni prodotte. La scelta delle etichette porta con sé pregiudizi e classificazioni soggettive che già di per sé potrebbero portare a forme di cd. "razzismo scientifico" [147].

---

[145] Sul punto v. K.A. GATES, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*, cit., p. 17 ss., in cui l'Autore sostiene che «*an individual face changes considerably not only with its surface movements, but also with aging, trauma, surgery, makeup, and lighting. Faces themselves change over time, and images captured of a face can be of highly variable quality. The variability faces across populations, as well the dynamic states of the individual and the range of images that can be rendered of a particular person, make automated facial recognition a very challenging technical problem*».

[146] Cfr. J. GALBALLY-P. FERRARA-R. HARAKSIM-A. PSYLLOS-L. BESLAY, *Study on Face Identification Technology for its Implementation in the Schengen Information System*, JRC-34751, luglio 2019, p. 58.

[147] Cfr. D. LESLIE, *Understanding bias in facial recognition technologies: an explainer*, in *The Alan Turing Institute*, 2020, p. 6; C. GARVIE, *Garbage In, Garbage Out: Face Recognition*

Ulteriori distorsioni potrebbero prodursi poi nella scelta delle categorie di dati che l'algoritmo deve elaborare o con cui gli algoritmi vengono allenati (cd. *training set*): si pensi a quei modelli di riconoscimento facciale in cui tale scelta viene stabilita dall'essere umano (cd. *handcrafted models*), così da considerare solamente alcuni tratti biometrici e non altri. Le immagini impiegate dovrebbero rispecchiare il più possibile la varietà delle informazioni fenotipiche delle persone [148].

Inoltre, tra gli elementi che influenzano le percentuali di falsi positivi e di falsi negativi, rientrano, come accennato, anche «la qualità e la risoluzione dell'immagine, il riflesso della luce, il movimento della persona ripresa, l'inclinazione e la posa del volto, ma anche l'età, il colore e le condizioni della pelle del soggetto, l'espressione, persino la pettinatura dei capelli o la presenza di trucco» [149].

Venendo alle metriche standardizzate utilizzate nella disciplina biometrica per la misurazione e la quantificazione degli errori, si fa generalmente riferimento a due categorie fondamentali: il "falso positivo" (*False Match Rate*, FMR) [150] e il "falso negativo" (*False Non-Match Rate*, FNMR) [151]. Trattasi di misure applicabili ai sistemi di verifica (1:1) che, tramite alcune semplificazioni di

---

on Flawed Data, in *Georgetown Law, Center on Privacy and Technology*, 16 maggio 2019; G. MOBILIO, *Tecnologie di riconoscimento facciale, Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, p. 35 ss.

[148] Sul punto si veda anche J. BUOLAMWINI-T. GEBRU, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proceedings of Machine Learning Research*, 81:1-15, 2018.

[149] Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 35-36.

[150] Detto anche *false match probability* o, in modalità di confronto 1:1, cd. "*false acceptance rate*". Invero, un ulteriore parametro fondamentale di un sistema biometrico è rappresentato dal cd. *Equal Error Rate* (EER), il cui valore è rappresentato dal punto di intersezione fra le curve del FMR e FNMR e costituisce una misura dell'accuratezza globale di un sistema biometrico. Cfr. COMITATO NAZIONALE PER LA BIOETICA, *L'identificazione del corpo umano: profili bioetici della biometria*, 26 novembre 2010. «*A biometric verification system makes two types of errors: 1) mistaking biometric measurements from two different persons to be from the same person (called false match) and 2) mistaking two biometric measurements from the same person to be from two different persons (called false nonmatch). These two types of errors are often termed as false accept and false reject, respectively. There is a tradeoff between false match rate (FMR) and false non match rate (FNMR) in every biometric system*». A.K. JAIN-A. ROSS-S. PRABHAKAR, *An Introduction to Biometric Recognition*, in *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 2004, p. 6.

[151] O in modalità di confronto 1:1, cd. "*false rejection rate*".

calcolo, possono essere utilizzate come parametro anche per i sistemi biometrici con finalità identificativa (1:N, 1:N+1) [152].

Il primo valore, invece, indica la probabilità attesa che due campioni appartenenti a due individui diversi siano riconosciuti come coincidenti [153]. La maggior parte dei casi in cui si verifica un FMR è dovuta ad una cattiva interazione dell'utente con il sensore del sistema e può essere facilmente risolta permettendo al soggetto di presentare nuovamente l'*input.* Tale errore risulta particolarmente critico nei sistemi di identificazione biometrica *one-to-many*, in cui l'associazione errata tra un individuo e un'identità preesistente compromette l'affidabilità dello strumento biometrico, minando la validità del processo di identificazione. Il rischio di falsi positivi aumenta proporzionalmente alla dimensione del database, con la possibilità che un soggetto venga erroneamente associato a un'identità non corrispondente.

Il secondo si riferisce alla probabilità che due campioni coincidenti e acquisiti dallo stesso utente, siano dichiarati erroneamente come provenienti da due individui diversi [154]. Questo tipo di errore può comportare l'esclusione indebita di un soggetto da un sistema di autenticazione o l'impossibilità di accesso a determinate risorse o aree protette, con implicazioni

---

[152] «*The accuracy of a biometric system in the identification mode can be inferred using the system accuracy in the verification mode under simplifying assumptions*». A.K. JAIN-A. ROSS-S. PRABHAKAR, *An Introduction to Biometric Recognition*, cit., p. 7.

[153] Per esempio, con riferimento all'utilizzo di sistemi biometrici con finalità identificativa «un "falso positivo" potrebbe verificarsi a causa di un errore nella raccolta o nella manipolazione reiterata dei dati genetici, nell'interpretazione distorta dei risultati dei *test*, oppure, nell'erronea segnalazione dei risultati di prova». M. MENDOLA, *Aspetti informatici delle prove biometriche. Il problema dei "Falsi positivi"*, cit. La formula matematica del valore di FMR è FMR(h) = $1 - \int_{s=h}^{\infty} p_n(s)ds$, ove, «*FMR is the rate that the decision is made that I matches T, while in fact I and T come from two different individuals where pn(s) is the non-match distribution between two samples as a function of the similarity score s*». A.I. AWAD-A.E. HASSANIEN, *Impact of Some Biometric Modalities on Forensic Science*, in A.K. MUDA *et al.* (eds.), *Computational Intelligence in Digital Forensics*, in *Forensic Investigation and Applications*, Springer, Cham, 2014.

[154] La formula matematica del valore di FNMR si trova espressa come FNMR(h)=1 – $\int_{s=-\infty}^{h} pm(s)\ ds$. Più nel dettaglio, «*FNMR is the rate that the decision is made that I does not match T, while I and T do in fact come from the same individual, where pm(s) is the match distribution between two samples as a function of the score s*». A.I. AWAD-A.E. HASSANIEN, *Impact of Some Biometric Modalities on Forensic Science*, in A.K. MUDA *et al.* (eds.), *Computational Intelligence in Digital Forensics*, cit., 555. La percentuale si trova anche indicata con la dicitura FRR ossia *False Rejection Rate.*

significative in contesti critici come la sicurezza aeroportuale o le procedure di verifica identitaria.

Attualmente sono disponibili strumenti estremamente avanzati che, impiegando dati di alta qualità [155], permettono di identificare un individuo attraverso immagini acquisite in ambienti controllati con un margine di errore ridotto allo 0,1% [156]. Tuttavia, non è possibile stabilire in modo assoluto o generalizzato quanto un sistema di riconoscimento sia accurato. Questa valutazione dipende da numerosi fattori che influenzano il livello di errore considerato "accettabile", a seconda del contesto di impiego, degli scopi che si intendono raggiungere tramite il riconoscimento e della possibilità di revisione critica da parte di un operatore umano qualificato.

5. *Il ruolo assunto dalle informazioni biometriche e le categorie di riferimento*

L'evoluzione della scienza biometrica e, più in generale, delle tecniche di trattamento dei dati fisici, fisiologici e comportamentali ha avuto un impatto significativo sulla concezione giuridica del corpo umano, trasformandolo in un'entità sempre più analizzabile, misurabile e digitalizzabile. L'avanzamento delle tecnologie di riconoscimento biometrico e di intelligenza artificiale ha reso il corpo non solo un soggetto di diritto, ma anche un oggetto di indagine e di prova in grado di fornire informazioni cruciali per l'accertamento della responsabilità penale, indipendentemente dall'atteggiamento collaborativo del suo titolare [157].

---

[155] Allo stato non ci sono standard per le metriche sulla qualità delle immagini facciali, al pari di quanto accade per le impronte digitali (ISO/IEC 29794-4:2017 *Information Technology – Biometric Sample Quality* – Part 4: *Finger image data*). Il NIST, agenzia governativa degli Stati Uniti, facente parte del Dipartimento del Commercio, incaricata di sviluppare standard, metriche e tecnologie di misurazione in diversi settori scientifici, tecnologici e industriali, ha elaborato uno standard nazionale per i dati biometrici utilizzabili a scopo di polizia, "ANSI/NIST ITL 1-2017".

[156] Cfr. P. GROTHER-M. NGAN-K. HANAOKA, *Face Recognition Vendor Test (FRVT). Part 2: Identification*, NIST, 2020, 4.

[157] Come sostiene C. BONZANO, *Gli accertamenti medici coattivi. Legalità e proporzionalità nel regime della prova*, Wolters Kluwer Cedam, Milano, 2017, p. 2 «la persona rappresenta

Questa trasformazione ha portato il corpo umano a essere concepito in termini dinamici e frammentabili, non più solo come un'unità organica inscindibile, ma come un insieme di dati e componenti autonomamente trattabili [158]. Il progresso scientifico ha, infatti, determinato una crescente destrutturazione del corpo che da entità fisica unitaria si è scomposto in una molteplicità di elementi – organi, tessuti, cellule, fluidi biologici – acquisendo, nel sistema giuridico e scientifico, una propria rilevanza autonoma. Questa frammentazione è divenuta ancora più evidente con l'avvento delle tecnologie digitali che hanno reso possibile la conversione del dato fisico in immagine digitalizzata, segnando una netta distinzione tra la materialità corporea originaria e la sua rappresentazione elettronica.

In ambito forense, tale evoluzione ha ampliato sensibilmente il potenziale probatorio del corpo umano. I dati biometrici, in particolare, hanno assunto una rilevanza centrale nei procedimenti penali, poiché consentono, tramite la loro comparazione, di associare, con una certa probabilità, l'identità di un soggetto e possono fornire elementi significativi ai fini della ricostruzione dei fatti. L'apporto scientifico ha reso possibile l'analisi di informazioni provenienti dal corpo umano che, fino a pochi anni fa, risultavano inaccessibili o non adeguatamente sfruttabili. Oltre ai tradizionali metodi di identificazione, attraverso impronte digitali e immagini del volto, oggi la tecnologia permette di elaborare dati biometrici con estrema precisione, quali le minime inflessioni della voce, la dinamica dei movimenti facciali, la postura, la biomeccanica dell'andatura e persino le reazioni fisiologiche involontarie [159]. Questi elementi possono fornire informazioni sulla partecipazione a determinati fatti di reato, contribuendo a delineare nuove prospettive nell'utilizzo delle prove biometriche nel processo penale. La digitalizzazione del corpo umano ha portato, pertanto, a una modalità del tutto inedita di investigazione [160].

---

da sempre – e dunque a prescindere dal sistema processuale di riferimento – la più allettante tra le prove e, al contempo, la più sensibile tra di esse: esprime un innato ed insopprimibile "interesse accertativo", che viene in rilievo sotto vari profili, al mutare dei quali cambiano i diritti individuali di riferimento e, per l'effetto, i modelli di tutela che debbono ritenersi operanti».

[158] Così, S. RODOTÀ, *Ipotesi sul corpo "giuridificato"*, in *Tecnologie e diritti*, il Mulino, Bologna, 1995, p. 204 e M. GIALUZ, *L'accesso al corpo tramite strumenti diagnostici*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2014, p. 289.

[159] Cfr. T. ALESCI, *Il corpo umano come fonte di prova*, Wolters Kluwer Cedam, Milano, 2017, p. 57 ss. e S. RODOTÀ, *Trasformazioni del corpo*, in *Pol. dir.*, 2006, p. 3 ss.

[160] Cfr. *ex multis* G. OATLEY-B. EWART, *Data mining and crime analysis*, in *Wiley*

Un aspetto emblematico di questa trasformazione è rappresentato dall'integrazione dei sistemi biometrici nei dispositivi digitali di largo consumo, fenomeno che segna una svolta significativa nell'interazione tra individuo e tecnologia. In particolare, gli *smartphone* di ultima generazione, ad esempio, sono dotati di modalità di sblocco basate sul riconoscimento facciale [161], tecnologia che trova applicazione anche nei *social media*, dove è utilizzata per facilitare il *tagging* nelle immagini e aumentare la visibilità degli utenti [162]. Anche nel settore dell'intrattenimento digitale, i sistemi di riconoscimento facciale vengono impiegati per migliorare l'interattività nelle *console* di gioco, contribuendo alla creazione di esperienze personalizzate [163]. Durante l'emergenza pandemica da Covid-19, tali sistemi sono stati impiegati per monitorare gli studenti durante gli esami a distanza [164], oppure per misurare la temperatura delle persone tra la folla, riconoscere soggetti tra coloro che non indossavano la mascherina e tracciare potenziali infetti [165].

Pertanto, l'ampio utilizzo da parte della popolazione di sistemi di intelligenza artificiale, incorporati in dispositivi digitali, ha generato una varietà di dati del tutto inedita che può avere un impatto decisivo per l'andamento delle indagini e per l'accertamento del reato e della responsabilità [166]. Infatti, da un

---

Interdisciplinary Reviews (WIREs): Data Minining and Knowledge Discovery, 1(2), 2011, p. 147-153; T. ALESCI, *Il corpo umano come fonte di prova*, cit., p. 57 ss.; S. QUATTROCOLO, *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Rev. Italo-espanola derecho procesal*, 2, 2018, p. 111.

[161] Cfr. https://support.apple.com/it-it/HT208108.

[162] Cfr. https://forbes.it/2020/02/18/social-media-octi-riconoscimento-facciale-ar-realta-aumentata/.

[163] Cfr. https://www.playstationzone.it/news-ps-vita/video-riconoscimento-facciale-per-ps-vita/.

[164] Cfr. A. DINI, *La tecnologia per combattere imbrogli e distrazioni negli esami online*, in *La Stampa*, 12 maggio 2020, reperibile su https://www.lastampa.it/topnews/tempi-moderni/2020/05/12/news/la-tecnologia-per-combattere-imbrogli-e-distrazioni-negli-esami-online-1.38835127.

[165] Cfr. M. VAN NATTA *et al.*, *The rise and regulation of thermal facial recognition technology during the Covid-19 pandemic*, in *Journal of Law and the Biosciences*, 7(1), 2020.

[166] Cfr. U. PAGALLO-S. QUATTROCOLO, *Fair Trial and the Equality of Arms in an Algorithmic Society*, in M.L. LABATE MANTOVANINI PADUA LIMA-J. GARCEZ GHIRARDI (eds.), *Global Law. Legal Answers for Concrete Challenges*, Juruà Editorial, Porto, 2018, p. 261 ss.; U. PAGALLO-S. QUATTROCOLO, *The impact of AI on criminal law, and its two fold procedures*, in W. BARFIELD-U. PAGALLO (eds.), *Research Handbook on the Law of Artificial Intelligence*, Edward Elgar, Chaltenham-Northampton, 12, 2018, p. 385-409; S. CONTI, *La legislazione in*

lato, gli strumenti informatici sono il mezzo per la commissione di reati e, dall'altro, le memorie dei dispositivi costituiscono altrettanti archivi di informazioni di cui gli organi inquirenti non possono più fare a meno per la ricostruzione del fatto [167]. In questo contesto, il dato biometrico acquisisce una centralità assoluta, rappresentando un'informazione unica e difficilmente alterabile, in grado talora di fornire elementi identificativi e probatori di elevata precisione. A questo proposito, occorre tenere presente che il trattamento del dato biometrico non è un'operazione uniforme, ma si articola attraverso modalità differenti che ne condizionano l'utilizzo e la rilevanza giuridica [168]. A seconda della modalità di acquisizione e della natura dell'informazione ottenuta, il tratto può presentarsi in diverse forme, variando in funzione del processo di elaborazione e della finalità di utilizzo. In sintesi, un dato biometrico può: consistere in una rappresentazione digitale del tratto o un *template*, frutto di procedimenti regolamentati di digitalizzazione, a partire da un campione biometrico grezzo (cd. "*dato trasformato/ convertito*") [169]; può essere ricavato da un'immagine o da un video ritraente un determinato dato biometrico (cd. "*dato ricavato*"); ovvero può essere generato da dispositivi automatici impiegati per un uso generico o commerciale (quindi inizialmente estranei al procedimento penale), quali assistenti domestici o dispositivi elettronici di rilevamento delle proprie caratteristiche fisiche, fisiologiche o comportamentali (cd. "*dato generato automaticamente*") [170].

Nei successivi capitoli [171], si procederà a una classificazione di tali dati rispetto alle tradizionali categorie probatorie, tenendo conto delle peculiarità

---

materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia, in *Informatica e diritto*, anno XLI, vol. XXIV, n. 1-2, 2015, p. 153-164.

[167] Cfr. G. CECANESE, *Le pre-investigazioni informatiche e i controlli sui social*, cit., p. 272; T. HUANG, Z. XIONG Z. ZHANGE, *Face Recognition Applications*, in Z.S. LI, A.K. JAIN (eds.), *The Handbook of Face Recognition*, Springer, New York, p. 617 ss.

[168] Cfr. il capitolo V.

[169] *Trasformato* in rappresentazione digitalizzata; *convertito* nel modello elettronico (cd. *template)*.

[170] Cfr. S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, p. 73; S. QUATTROCOLO, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, 2020, p. 121 ss. e S. QUATTROCOLO, *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Rev. Italo-espanola derecho procesal*, 2, 2018, p. 107 ss.

[171] Cfr. il capitolo V.

che caratterizzano l'evidenza digitale e la specificità dei dati biometrici. L'eterogeneità che connota le modalità di trattamento dei dati biometrici si riflette direttamente sul grado di attendibilità e precisione del risultato ottenuto, il quale risulta fortemente influenzato da molteplici fattori. Tra questi, assumono rilievo primario la qualità della fase di acquisizione del dato, la metodologia tecnica adottata per la sua successiva elaborazione e, infine, l'efficacia dei protocolli di verifica impiegati per garantire la conservazione della sua integrità e la non alterazione del contenuto informativo. Nel contesto procedimentale, la modalità di acquisizione e trattamento del dato biometrico riveste certamente un ruolo determinante ai fini della sua ammissibilità probatoria, potendo incidere altresì sulla valutazione della sua attendibilità [172]. La natura di questi dati impone l'adozione di criteri di validazione scientifica rigorosi, al fine di garantire che il loro utilizzo sia conforme agli standard metodologici riconosciuti.

Si anticipa che l'approccio non può essere statico: la natura multiforme del dato digitale e la complessità intrinseca dei tratti biometrici suggeriscono di adottare una prospettiva elastica e adattabile, in grado di recepire le continue innovazioni tecnologiche e di evitare generalizzazioni aprioristiche [173]. Qualsiasi delimitazione epistemologica eccessivamente dettagliata rischierebbe, infatti, di risultare immediatamente superata, considerata la rapidità con cui mutano le tecnologie di acquisizione e trattamento dei dati biometrici.

Come visto, il dato, per sua stessa natura, presenta livelli di complessità differenti, a seconda della finalità per cui è stato acquisito, del contesto in cui viene trattato e del tipo di informazione estratta [174]. Tale versatilità impone un approccio metodologico che tenga conto delle specificità proprie di ciascuna categoria di dato biometrico digitalizzato senza forzature concettuali che potrebbero ridurre l'accuratezza dell'inquadramento giuridico e pregiudicare la sua adeguata regolamentazione. L'analisi dovrà dunque muoversi entro uno schema teorico flessibile, in grado di cogliere le implicazioni giuridiche, forensi e tecnologiche di questi dati e di individuare soluzioni normative e procedurali che ne garantiscano un utilizzo conforme ai diritti fondamentali.

---

[172] Cfr. il capitolo V, 6.1.

[173] Cfr. M. DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012, p. 441.

[174] Cfr. S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, cit., p. 226.

Capitolo III
L'impatto trasversale sui diritti fondamentali

SOMMARIO: 1. La tecnologia di riconoscimento facciale e le garanzie processuali coinvolte. – 2. Il riconoscimento facciale automatizzato e la libertà personale. – 3. Nuovi e più labili confini tra gli artt. 13 e 24 Cost.: il *nemo tenetur se detegere* nel quadro delle nuove intrusioni nella sfera personale. – 4. Il trattamento del dato biometrico digitalizzato nel rispetto del diritto alla riservatezza. – 4.1. Un'ipotesi specifica di trattamento: il processo decisionale automatizzato. – 4.2. Il perimetro del trattamento tra i principi di limitazione della finalità e di minimizzazione dei dati. – 4.3. Approcci giurisprudenziali stranieri all'impatto del riconoscimento facciale sul diritto alla riservatezza: il procedimento inglese *Ed Bridges (R)* c. *The Chief Constable of South Wales Police*. – 4.4. (Segue) L'affaire *Glukhin c. Russia*: prime indicazioni da Strasburgo. – 5. I rischi per la parità delle armi. – 5.1. I sistemi di intelligenza artificiale tra trasparenza e spiegabilità dei risultati: i rimedi tecnici indispensabili al diritto di difesa e al contraddittorio. – 5.2. Tra interpretabilità e certificazione del metodo. – 5.3. I criteri di equità e di legalità.

1. *La tecnologia di riconoscimento facciale e le garanzie processuali coinvolte*

Inquadrato il funzionamento delle tecnologie di riconoscimento facciale, occorre ora stabilire quali siano le garanzie fondamentali su cui esse sono potenzialmente in grado di incidere e con quali modalità ciò possa avvenire[1]. Tra le particolarità che contraddistinguono questi strumenti, infatti, vi è la capacità di condizionare contestualmente e trasversalmente una serie di diritti e libertà fondamentali[2]. Come è stato osservato, «tanto queste

[1] Come suggerito da C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Dir. pubbl. comp. eur.*, f.s., 2019, p. 102 ss., FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019.

[2] Per una ricognizione completa sul tema cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, p. 57 ss.

tecnologie sono versatili, quanto possono combinare limitazioni a diritti e libertà in una pluralità di dimensioni»[3]. Da diversi anni l'Agenzia UE per i diritti fondamentali[4] e il Garante europeo per la protezione dei dati personali[5] hanno sollevato la questione riguardante i potenziali rischi derivanti dall'impiego della tecnologia di riconoscimento facciale, specie se utilizzata *in tempo reale*, in luoghi aperti al pubblico e in occasione di eventi o manifestazioni, potendo le persone sottoposte a mezzi di sorveglianza di massa «*change their behaviour, withdrawing from social life, not visiting central places under surveillance, avoiding train stations or declining to attend cultural, social or sports events*»[6]. Il ricorso a questa tecnologia può essere talmente intrusivo in particolari contesti sociali, da scoraggiare e dissuadere addirittura l'esercizio di diritti o libertà fondamentali (cd. *chilling effect*)[7]. In questa prospettiva, «l'impiego degli strumenti di riconoscimento facciale *real time* (…) ha finito per offrire un'argomentazione in più a quanti sostengono da tempo che le tecnologie di videosorveglianza in generale e, data la loro maggiore intrusività, quelle di identificazione biometrica basate sui tratti caratteristici del volto, in particolare, possono determinare nei consociati un atteggiamento di auto-censura»[8].

A maggior ragione, quando questa tecnologia di riconoscimento venga impiegata in taluni settori e con certe finalità, come quelle di indagine e repressione dei reati, si pongono delicati problemi di bilanciamento tra le esigenze di indagine penale e la tutela di alcune garanzie fondamentali[9].

---

[3] Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 58.

[4] Cfr. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27 novembre 2019, p. 29 ss., https://fra.europa.eu/en/publication/2019/facial-recognition.

[5] Cfr. *"Facial recognition: A solution in search of a problem?"*, https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en.

[6] Cfr. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., p. 20.

[7] Cfr. M. BÜCHI, *Chilling Effects of Profling Activities: Mapping the Issues*, in *Computer Law & Security Review*, 36, 2020.

[8] Cfr. C. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *Leg. pen.*, 11 dicembre 2021, p. 12.

[9] Su questo, tra gli altri, cfr. S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Springer, Cham, 2020; A. ZAVRSNIK, *Criminal justice, artificial intelligence systems and human rights*, in *ERA Forum*, 2020, p. 575; C. CESARI, *L'impatto delle nuove tecnologie sulla giustizia penale –*

Al fine di dare conto di tale intrusività, si fornirà una descrizione di come la tecnologia si atteggi rispetto ad alcuni diritti fondamentali rilevanti per il contesto processuale penale, intesi sia nei loro significati più tradizionali, sia nelle accezioni più estensive.

Il tema della tutela dei diritti inviolabili della persona impone un costante riferimento alla giurisprudenza costituzionale e sovranazionale che ne ha progressivamente modellato i contenuti e, conseguentemente, gli ambiti di tutela. La tendenza che si coglie è quella di abbracciare un'interpretazione "evolutiva" dei diritti e delle libertà fondamentali, «funzionale al riconoscimento di nuove prerogative minacciate dall'impiego dei moderni mezzi di controllo» [10]. Emerge la necessità di una rilettura più ampia e dai contorni ancora non ben definiti dei diritti inviolabili. L'obiettivo diventa quello di indagare se e come la tecnologia di riconoscimento facciale sia in grado di insidiare alcuni diritti e libertà, anche nelle loro più complesse sfaccettature. A questo proposito, data la tendenziale novità della problematica affrontata, è utile misurarsi anche con le esperienze maturate in altri ordinamenti nazionali. In particolare, si vedrà come istituti e principi posti a tutela della protezione dei dati personali abbiano già messo alla prova la propria tenuta nel caso di un contenzioso verificatosi nel Regno Unito; da questo sarà possibile ricavare numerosi spunti sulle condizioni per l'utilizzo di tali strumenti anche nell'esperienza italiana. Una volta colto l'impatto sui diritti fondamentali, nei capitoli successivi, ci si soffermerà sulla regolamentazione giuridica attualmente disponibile al fine di vagliarne l'adeguatezza [11].

---

un orizzonte denso di incognite, in *Rev. Bras. de Direito Processual Penal*, 5(3), 2019, p. 1174; A. SIMONCINI, *L'algoritmo incostituzionale:intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 1, 2019, p. 65; S. MARCOLINI, *Regole di esclusione e nuove tecnologie*, in *Criminalia*, 1, 2006, p. 391; L. PARLATO, *Libertà della persona nell'uso delle tecnologie digitali*, in *Diritti della persona e nuove sfide del processo penale*, Giuffrè, Milano, 2019, p. 205 ss.; G. DI PAOLO, *"Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione*, Cedam, Padova, 2008, p. 1 ss. e S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 6.

[10] Cfr. F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Wolters Kluwer Cedam, Milano, 2020, p. 47.

[11] Cfr. i capitoli IV e V.

2. *Il riconoscimento facciale automatizzato e la libertà personale*

Lo studio della progressiva "intrusione" nel corpo dell'individuo per mezzo dell'impiego sistematico di software automatizzati di riconoscimento a fini processuali non può prescindere da una ricostruzione preliminare circa il livello di tutela offerto alla libertà personale dal nostro ordinamento [12].

Per valutare se vi sia una correlazione diretta fra l'impiego di tecnologie di riconoscimento facciale e la garanzia della libertà personale, *lato sensu* intesa, bisogna innanzitutto guardare al bene giuridico di riferimento e alla portata della tutela riconosciuta nell'art. 13 Cost. In questo perimetro, la libertà personale è stata inizialmente intesa come libertà dalle sole *coercizioni fisiche* [13], ossia quelle che comportano un *pati* corporeo da parte di chi le subisce [14]. Secondo questa lettura iniziale non vi rientrerebbero «tutte quelle misure che non comportano una "privazione" della libertà personale, ma una mera limitazione della stessa, quali, ad esempio, il divieto di espatrio e tutte le altre misure prescrittive nel nostro ordinamento» [15]. Gli atti che incidono solo sull'aspetto esteriore dell'individuo o che pongono limitazioni lievi e momentanee, non sarebbero ascrivibili all'art. 13 Cost. Conseguentemente, tali atti non richiederebbero l'osservanza della riserva di legge assoluta, né della riserva di giurisdizione, trattandosi di interventi che non incidono in modo significativo nella sfera individuale [16].

---

[12] Per una riflessione sistematica, cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, p. 57 ss.

[13] Cfr. Corte cost., 23 giugno 1956, n. 2, in *www.cortecostituzionale.it*, 1956, p. 561 ss.

[14] Cfr. G. AMATO, *Commento all'art. 13 Cost.*, in G. BRANCA (a cura di), *Commentario alla Costituzione*, Zanichelli, Bologna, 1977, p. 44 ss.; V. DI NICOLA, *La libertà personale dell'imputato tra regole smesse, disciplina attuale e sistema futuro*, Boccia, Salerno, 1989, p. 11 ss.; F. CARNELUTTI, *Principi del processo penale*, Morano, Napoli, 1960, p. 175 ss.; C. BONZANO, *Gli accertamenti medici coattivi*, Wolters Kluwer Cedam, Milano, 2017, p. 61.

[15] Cfr. P. SPAGNOLO, *Libertà personale e processo*, in *In onore di Mario Chiavario*, in *Leg. pen.*, 19 ottobre 2020, p. 165; ID., *Il Tribunale della libertà. Tra normativa nazionale e normativa internazionale*, Giuffrè, Milano, 2008 e M. PISANI, *sub art. 5. Diritto alla libertà e alla sicurezza*, in S. BARTOLE-B. CONFORTI-G. RAIMONDI (a cura di), *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, Cedam, Padova, 2001, p. 117 ss.

[16] Cfr. Corte cost. nn. 30/1962, 13/1972 e 23/1975 in cui la Corte afferma che «l'ambito precettivo della norma costituzionale, diretta a difendere l'individuo di fronte alla potestà coattiva dello Stato, non comprende ogni violazione o limitazione della libertà personale, cui

Un'interpretazione alternativa, invece, intende la libertà personale come la disponibilità non solo fisica, ma anche psichica e morale, di sé stessi, ovvero come espressione della volontà autodeterminativa dell'essere umano [17]. In questa prospettiva, la libertà personale si configura come un diritto inviolabile che non si esaurisce nella protezione della mera integrità fisica e nella possibilità di movimento, ma si estende alla piena gestione della propria identità, integrità mentale ed espressione individuale [18]. Tale lettura è stata adottata anche dalla Corte costituzionale che, in alcune pronunce, pur escludendo che la coazione fisica comporti sempre necessariamente una contrazione della libertà personale, ha affermato che tale diritto possa considerarsi compresso anche attraverso provvedimenti che comportino «una menomazione o mortificazione della dignità e del prestigio della persona» [19]. Questo orientamento ha posto particolare enfasi sul criterio della "degradazione giuridica dell'individuo", riconoscendo che la libertà personale non è riducibile alla sola tutela dall'arbitraria privazione della libertà fisica, ma implica anche la protezione della dignità umana, intesa quale fondamento essenziale del-

può essere sottoposto in vario modo il cittadino nello svolgimento della sua attività, ma soltanto gli atti lesivi di quel diritto che trae la sua denominazione tradizionale dall'*habeas corpus* inteso come autonomia e disponibilità della propria persona».

[17] Cfr. A. BARBERA, *Pari dignità sociale e valore della persona umana nello studio del diritto di libertà personale*, in *Iustitia*, 1962, p. 129 ss.; G. AMATO, *Art. 13*, in *Comm. Cost. Branca*, Zanichelli-Foro italiano, Bologna-Roma, 1977, p. 47 ss.; P. BARILE, *Diritti dell'uomo e libertà fondamentali*, il Mulino, Bologna, 1984, p. 111; A. PACE, voce *Libertà personale (dir. cost.)*, in *Enc. dir.*, XXIV, Milano, 1974, p. 287 ss.; P. FELICIONI, *La prova del Dna nel procedimento penale. Profili sistematici, dinamiche probatorie, suggestioni mediatiche*, Giuffrè, Milano, 2018, p. 180 ss.; T. ALESCI, *Il corpo umano fonte di prova*, cit., p. 13 e 18; L. PARLATO, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, in *Proc. pen. giust.*, 2020, p. 298; da ultimo, A. CHELO, *La tutela della libertà morale nella formazione della prova penale*, Wolters Kluwer Cedam, Padova, 2025.

[18] Si parla di "personalità morale" e di "dignità sociale" della persona. cfr. A. BARBERA, *I principi costituzionali della libertà personale*, Giuffrè, Milano, 1967, p. 119 ss.

[19] Cfr. Corte cost. 3 luglio 1956, n. 11 e Corte cost. 30 giugno 1964, n. 68, in *www.corte costituzionale.it.* Risulta evidente l'influenza esercitata da alcuni atti internazionali. Si pensi al Preambolo della Dichiarazione universale dei diritti umani del 1948, in cui si stabilisce che «nel riconoscimento della dignità inerente a tutti i membri della famiglia umana e dei diritti uguali ed inalienabili di tutti gli esseri umani, che da questa discendono, può rinvenirsi "il fondamento della libertà, della giustizia e della pace nel mondo"». Ugualmente nel preambolo del Patto sui diritti civili e politici del 1966, ratificato in Italia con la legge 25 ottobre 1977, n. 881, in *G.U.* 7 dicembre 1977, che riconosce la dignità inerente a tutti i membri della famiglia umana e (…) i loro diritti, uguali ed inalienabili, come «fondamento della libertà, della giustizia e della pace nel mondo».

l'autonomia individuale[20]. Per ravvisare una violazione della libertà personale, secondo questa interpretazione, pur tenendo conto del criterio distintivo tra misure incidenti e misure non incidenti sulla libertà personale[21], non dev'esserci per forza una coercizione fisica, essendo sufficiente «una menomazione o mortificazione della dignità, tale da poter essere equiparata a quell'assoggettamento all'altrui potere in cui si concreta la violazione dell'*habeas corpus*»[22].

L'interpretazione di questa garanzia ha poi trovato un punto di svolta diverso, ma cruciale, nell'ambito della giurisprudenza costituzionale con la sentenza n. 238 del 1996 che ha assunto un ruolo dirimente nel delineare il perimetro entro cui il legislatore è chiamato a esercitare la propria discrezionalità nella definizione dei «casi e modi» in cui può essere autorizzata un'incisione sulla libertà personale da parte del giudice[23]. Secondo la Corte

---

[20] Cfr. Corte cost. 30 giugno 1964, n. 68, cit.: «l'ammonizione – si sostiene nella pronuncia – […] si risolve in una sorta di degradazione giuridica in cui taluni individui, appartenenti a categorie di persone che la legge presume socialmente pericolose, magari designati come tali dalla pubblica voce, vengono a trovarsi per effetto di una pronuncia della pubblica autorità». Sul nesso tra "degradazione" della persona e libertà morale della stessa cfr. anche G. AMATO, *Art. 13*, in *Comm. cost.*, cit., p. 47 ss.

[21] Cfr. Corte cost. 22 marzo 1962, n. 30, in *www.cortecostituzionale.it.* Con riferimento ai rilievi fotodattiloscopici disciplinati dall'art. 4 TULPS la Corte ha stabilito che: «(…) i rilievi descrittivi, fotografici ed antropometrici, e sempre i rilievi dattiloscopici (almeno nella forma in cui sono attualmente eseguiti in ogni paese del mondo), non importano menomazione della libertà personale, anche se essi possano talvolta richiedere una momentanea immobilizzazione della persona per descriverne o fotografarne o misurarne gli aspetti nelle parti normalmente esposte all'altrui vista o richiedere una momentanea costrizione tendente alla fissazione delle impronte digitali».

[22] Cfr. Corte cost. 29 maggio 1995, n. 210, in *www.cortecostituzionale.it*., Corte cost. 22 marzo 2001, n. 105, in *www.cortecostituzionale.it*. Cfr. G. AMATO, *Individuo e autorità nella disciplina della libertà personale*, Giuffrè, Milano, 1967, p. 105; P. BISCARETTI DI RUFFIA, voce *Habeas corpus*, in *Enc. dir.*, XIX, Milano, 1970, p. 941; A.M. DE CESARIS, voce *Habeas corpus*, in *Enc. Treccani*, XIX, Roma, 1991; M. RUOTOLO, voce *Habeas corpus* in M. FLORES (diretto da), *Diritti umani. Cultura dei diritti e dignità della persona nell'epoca della globalizzazione*, *Dizionario*, vol. II, Utet, Torino, 2007, p. 695 ss.; M. DANIELE, *Habeas Corpus. Manipolazioni di una garanzia*, Giappichelli, Torino, 2017, p. 3 ss.; V. GREVI, voce *Libertà personale dell'imputato*, in *Enc. dir.*, XXIV, Giuffrè, Milano, 1974, p. 316; V. GREVI, *Libertà personale dell'imputato e Costituzione*, Giuffrè, Milano, 1976, p. 1 ss.; V. GREVI (a cura di), *La libertà personale dell'imputato. Verso il nuovo processo penale*, Cedam, Padova, 1989; M. CHIAVARIO, *Processo e garanzie della persona*, II, *Le garanzie fondamentali*, Giuffrè, Milano, 1984, p. 299; T. ALESCI, *Il corpo umano fonte di prova*, cit., p. 11.

[23] Come noto, alla luce del diritto vivente, la Corte ha dichiarato l'illegittimità costituzionale dell'art. 224 c.p.p., nella parte in cui attribuiva al giudice il potere di disporre

occorre una disciplina normativa di riferimento chiara, puntuale e rigorosa quale presupposto imprescindibile per legittimare l'esecuzione di accertamenti coattivi sulla persona. L'intervento del giudice delle leggi ha dunque reso evidente la necessità di subordinare ogni limitazione della libertà personale, anche quando funzionale al perseguimento di finalità probatorie, a una base normativa chiara e tassativa, che ne definisca con rigore presupposti, ambito applicativo e modalità esecutive [24].

Venendo al nucleo problematico oggetto della presente trattazione, l'obiettivo primario dell'analisi consiste nel verificare se l'utilizzo della tecnologia di riconoscimento facciale nel contesto del procedimento penale, possa determinare effetti giuridici e materiali assimilabili – in termini di incidenza sui diritti fondamentali – a quelli propri delle misure coercitive soggette alla riserva di legge e di giurisdizione ai sensi dell'art. 13 Cost., secondo un'interpretazione costituzionalmente orientata e tendenzialmente estensiva della nozione di "libertà personale". Mentre il ricorso alle tecniche di riconoscimento facciale non solleva particolari criticità con riferimento alla libertà personale intesa nell'accezione più tradizionale, di assenza di coercizioni fisiche [25], l'impiego delle stesse, nella modalità *in tempo reale*, potrebbe implicare taluni rischi nel significato più ampio di "libertà morale" o "dignità sociale". Proprio con riguardo alla libertà morale, l'art. 188 c.p.p. afferma che «non possono essere utilizzati, neppure con il consenso della persona interessata, metodi o tecniche idonei a influire sulla libertà di autodeterminazione o ad alterare la capacità di ricordare e di valutare i fatti». Tale divieto impedisce il ricorso a strumenti che influiscono sulla facoltà di reagire liberamente agli stimoli, o che siano idonei ad alterare la capacità di valutare i fatti, o più in generale, riconducibili a manipolazioni psichiche atte

misure coattive incidenti sulla libertà personale dell'indagato, dell'imputato o di terzi nell'ambito delle operazioni peritali, in assenza di una espressa previsione normativa che ne definisse puntualmente i presupposti applicativi, ovvero «nei casi e nei modi previsti dalla legge». La norma censurata conferiva infatti un potere ampiamente discrezionale al giudice, privo di una chiara delimitazione oggettiva, determinando così una potenziale vulnerabilità per i diritti fondamentali della persona. Cfr. Corte cost. 9 luglio 1996, n. 238, in *www.cortecostituzionale.it*.

[24] Cfr. T. ALESCI, *Il corpo umano fonte di prova*, cit., p. 18 e L. PARLATO, *Libertà della persona nell'uso delle tecnologie digitali*, in L. KALB (a cura di), *Diritti della persona e nuove sfide del processo penale*, Giuffrè, Milano, 2019, p. 216.

[25] Ovviamente fatto salvo il caso in cui il rifiuto alla sottoposizione al riconoscimento faccia scattare l'uso della forza. Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 82.

a indurre in errore o indebolire la consapevolezza dell'interessato[26]. In tal senso, le illustrate modalità applicative del riconoscimento facciale potrebbero produrre una condizione e uno stato psicologico di "assoggettamento" conseguente ad un'attività di acquisizione diretta nei confronti del singolo individuo, in ragione di una sua particolare condotta, ovvero della sua presenza in una determinata area geografica; infatti, come già affermato, l'impiego dello strumento in questione è in grado di indurre le persone a cambiare comportamento e abitudini, pur di venir meno a simili forme di controllo. Peraltro, vale la pena di considerare che, qualora questo sistema fosse attivato in modo occulto, paradossalmente, potrebbe implicare un minor grado di intrusività sul piano esperienziale, configurandosi come una forma di controllo invisibile che, proprio in virtù della sua impercettibilità, eviterebbe di incidere direttamente sulla capacità di autodeterminazione dell'individuo.

La questione risulta più complessa nel caso in cui tali strumenti siano impiegati *a posteriori*. Vien da domandarsi se l'utilizzo di siffatte tecniche di riconoscimento facciale, durante le operazioni attinenti all'identificazione in senso stretto, da parte della polizia giudiziaria, possa eventualmente ledere la libertà personale dell'interessato e in quali termini. La sola sottoposizione a processi automatizzati di riconoscimento, non implicando un intervento coercitivo, né un'intrusione diretta nella libertà morale, non sembrerebbe giustificare l'estensione della garanzia di cui all'art. 13 Cost. nella sua accezione più ampia[27]. Parrebbe dunque legittima, almeno per il raggiungimento delle finalità previste nell'art. 349 c.p.p.[28], la costrizione che vede l'interessato partecipare non attivamente, ma come mero oggetto di un *pati*, analogamente a quanto accade in relazione ai rilievi fotografici o per il prelievo di impronte digitali o materiale organico (comma 2).

Di avviso contrario sono stati il Comitato e il Garante europeo per la protezione dei dati personali, i quali hanno sostenuto che, sul piano dei diritti fondamentali, l'invasività del trattamento non dipenda dal fatto che l'identificazione sia eseguita *in tempo reale* o *a posteriori*[29]. Lo strumento in

---

[26] Cfr. anche gli artt. 64, comma 2, 220, comma 2, c.p.p.

[27] Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale.*, cit., p. 88 e M. TORRE, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. e proc.*, 8, 2021.

[28] Più ampiamente, cfr. il capitolo V, § 4.

[29] Cfr. EDPB-GEPD, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale)*, 18 giugno 2021, p. 13.

entrambe le modalità applicative, se utilizzabile, per esempio, immediatamente dopo una manifestazione di protesta, può avere un profondo effetto dissuasivo sull'esercizio della libertà personale [30]. La differenza fra i due impieghi sarebbe essenzialmente tecnica e sarebbe unicamente circoscritta al momento in cui si svolgono le operazioni di comparazione e di riconoscimento [31].

Una violazione del disposto dell'art. 188 potrebbe essere più verosimilmente profilabile in caso di ricorso a tecniche di analisi facciale volte alla ricostruzione della personalità del soggetto, finalizzate ad accertare se questi stia o meno dicendo la verità [32]. Infatti, lo strumento sarebbe in grado di influire sulla libertà morale del soggetto destinatario della misura [33], incidendo in modo diretto sulla sua capacità di autodeterminarsi nel contesto processuale. Inoltre, come visto, l'efficacia scientifica di tali strumenti rimane fortemente contestata. Numerose ricerche nell'ambito della psicologia forense e delle neuroscienze cognitive hanno dimostrato l'assenza di un nesso univoco, stabile e replicabile tra le micro-espressioni facciali e la menzogna [34].

In conclusione, quindi, si può affermare che l'art. 188 c.p.p. rappresenta certamente un ostacolo per l'impiego nel procedimento di metodiche di riconoscimento facciale finalizzate alla rilevazione delle emozioni. Per quanto riguarda, invece, metodiche più basilari, si ritiene importante richiamare

---

[30] Su questo punto v. L. CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, in *Riv. it. dir. e proc. pen.*, 1, 1 marzo 2024, p. 233; F. PAOLUCCI, *From Global Standards to Local Safeguards: The AI Act, Biometrics, and Fundamental Rights*, in *SSRN*, 2024,; A. SCHRÖDER, *"Real-time" versus "post" remote biometric identification systems under the AI Act*, ALTI Forum, 14 ottobre 2022; N. MENÉNDEZ-G. MOBILIO, *Between the prohibited risks and high risks: the regulation of facial recognition technology*, in O. POLLICINO-F. DONATI-G. FINOCCHIARO-F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, Giuffrè, Milano, 2025, p. 214.

[31] Cfr. A. KAK (ed.), *Regulating Biometrics: Global Approaches and Urgent Questions*, in *AI Now Institute*, 2020.

[32] Per un approfondimento cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 38 ss.

[33] Da intendersi come il diritto «di formare senza costrizioni la propria volontà e di muovere il proprio comportamento esteriore in conformità delle spinte psichiche interne, senza intromissioni e senza la sottoposizione coatta ad introspezioni che ne svelino il concreto funzionamento». L. SCOMPARIN, *La tutela del testimone nel processo penale*, Cedam, Padova, 2000, p. 2.

[34] Cfr. più ampiamente il capitolo II, § 4.5.1.

l'attenzione sul possibile contrasto tra la norma codicistica e l'impiego del *real time face recognition*, in ragione della capacità di interferenza con la libertà di autodeterminazione. Residuale, ma non da ignorare, l'eventualità che anche i sistemi *post remote* possano, in uno scenario di utilizzazione molto diffusa, determinare effetti di coercizione morale sulla collettività.

3. *Nuovi e più labili confini tra gli artt. 13 e 24 Cost.: il* nemo tenetur se detegere *nel quadro delle nuove intrusioni nella sfera personale*

Al di là degli approdi raggiunti sia dalla normativa interna, sia dalla giurisprudenza europea in tema di acquisizione coattiva di prove materiali, un'ulteriore traiettoria interpretativa si potrebbe seguire se si valorizzasse un'accezione ancora più ampia di libertà morale, intesa come «forma di autodeterminazione nelle proprie scelte difensive e degli atteggiamenti processuali "sul fatto proprio"»[35], rispetto alle fasi di acquisizione ed estrazione dei *punti di repere* dai volti[36]. Non si può infatti negare che, a livello teorico, il *privilege against self-incrimination*, se interpretato in un'accezione più ampia, non si limiterebbe alla mera facoltà di non rendere dichiarazioni nell'ambito del processo penale, ma potrebbe estendersi sino a comprendere il diritto a non compiere atti corporei che, direttamente o indirettamente, possano contribuire alla formazione della prova[37]. In questa prospettiva, la sottoposizione forzata – sebbene pacificamente ammessa in numerose altre situazioni – potrebbe idealmente configurarsi come una potenziale violazione

---

[35] Cfr. *ex multis* M. SCAPARONE, *sub art. 24, c. 2, Cost.*, in *Comm. Cost. Branca*, Zanichelli-Foro italiano, Bologna-Roma, 1981; V. GREVI, *Alla ricerca di un processo penale "giusto". Itinerari e prospettive*, Giuffrè, Milano 2000, p. 203 ss.; V. GREVI, *Nemo tenetur se detegere: interrogatorio dell'imputato e diritto al silenzio nel penale italiano*, Giuffrè, Milano, 1972, p. 9; G.P. VOENA, voce *Difesa: III) difesa penale*, in *Enc. giur.*, Roma, 1989, p. 17; G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., p. 90.

[36] Cfr. L. PARLATO, *Il riconoscimento facciale: vantaggi e insidie alla luce della giurisprudenza della corte EDU*, in P. DI SIMONE-A. MANGIARACINA-L. PARLATO (a cura di), *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, Palermo University Press, Palermo, 2023, p. 100 ss.

[37] Cfr. M. SCAPARONE, *Elementi di procedura penale. I principi costituzionali*, Giuffrè, Milano, 1999, p. 123.

di tale diritto, nella misura in cui il volto dell'individuo venga trattato non solo come tratto fisiologico, ma come una vera e propria fonte di prova, suscettibile di generare informazioni rilevanti, quali quelle che conseguono all'elaborazione dell'immagine a fini identificativi.

D'altra parte, va anche ricordato che l'ordinamento non consente né di celare completamente il proprio volto (in luogo pubblico) [38], né di astenersi dal fornire le proprie generalità (obbligo, peraltro, penalmente sanzionato) [39]. Cosicché, a ben vedere, in questa prospettiva, il problema sul quale pare opportuno richiamare l'attenzione non è tanto il dovere di mostrare il proprio volto – incontrovertibile perlomeno alla luce dei precedenti richiami – quanto, piuttosto, la successiva elaborazione a fini identificativi del dato biometrico che dal volto medesimo si ricava. In altri termini, la garanzia in gioco potrebbe consistere nella circoscritta facoltà di non rendere il proprio volto disponibile per le operazioni tecniche di riconoscimento facciale [40].

Non risolutiva, ai fini della tematica qui evidenziata, è la giurisprudenza di Strasburgo. Infatti, guardando agli orientamenti in materia di "*nemo tenetur se detegere*", rileva solamente il profilo dell'acquisizione di prove connesse direttamente alla volontà dell'imputato [41]. In tale prospettiva, l'unica ipotesi in cui il *privilege* sopra menzionato sarebbe violato è quella in cui le modalità coercitive impiegate («*the nature and the degree of the compulsion*» [42]) ledano l'art. 3 Conv. eur. dir. uomo, essendo qualificabili come forme di tortura o trattamenti inumani e degradanti [43]. Come è noto, è stata infatti delineata una distinzione tra dichiarazioni ed elementi di prova di

---

[38] Cfr. gli artt. 85 r.d. 18 giugno 1931, n. 773 e 5 della legge 22 maggio 1975, n. 152.

[39] Cfr. gli artt. 495, 495-*ter*, 496 e 651 c.p.

[40] Cfr. F. CARNELUTTI, *Principi del processo penale*, Giuffrè, Milano, 1960, p. 175; M. SCAPARONE, *Elementi di procedura penale. I principi costituzionali*, cit., p. 123.

[41] La Corte ha ripetutamente affermato che il diritto di non auto-incriminarsi non si estende all'uso, in un procedimento penale, di dati che esistono indipendentemente dalla volontà del sospettato, come documenti raccolti in base ad un mandato, prelievi di sangue, urine e tessuti per un'analisi del DNA. Così, per la prima volta, C. eur. 17 dicembre 1996, *Saunders c. Regno Unito*, in M. DE SALVIA-V. ZAGREBELSKY, *Diritti dell'uomo e libertà fondamentali*, Giuffrè, Milano, 2007, p. 537.

[42] Cfr. C. eur. 15 giugno 1999, *Tirado Ortiz e Lozano Martin c. Spagna*, App. n. 43486/98, C. eur. 11 luglio 2006, *Jalloh c. Germania*, App. no. 54810/00.

[43] C. eur. 11 luglio 2006, *Jalloh c. Germania*, in *Cass. pen.* 2006, p. 3843 s. Su tale pronuncia cfr. *ex multis*, A. BALSAMO, *Il contenuto dei diritti fondamentali*, in R.E. KOSTORIS (a cura di), *Manuale di Procedura Penale Europea*, Giuffrè, Milano, 2017, p. 174, G. UBERTIS, *Attività investigativa e prelievo di campioni biologici*, in *Cass. pen.*, 2008, p. 9 s.

natura materiale che sussistono indipendentemente dalla volontà dell'imputato e che questi potrebbe peraltro fornire, anche inconsapevolmente, nel corso del procedimento. Se, da un lato, il principio del *nemo tenetur* tutela il soggetto dall'obbligo di rendere dichiarazioni contro sé stesso, dall'altro lato, esso non si estende automaticamente a tutte le acquisizioni probatorie che prescindono da un'adesione consapevole e attiva da parte dell'interessato.

Da questo punto di vista, uno dei casi più problematici è forse rappresentato dall'utilizzo di tecnologie biometriche per lo sblocco di dispositivi informatici, come lo *smartphone*, il *tablet* o il computer [44]. La richiesta da parte della polizia giudiziaria di attivare un dispositivo attraverso il riconoscimento facciale, l'impronta digitale o il riconoscimento vocale, solleva interrogativi complessi in merito alla compatibilità di tali procedure con il sopra menzionato diritto a non auto-incriminarsi. Riconosciuto che l'attivazione del dispositivo tramite un dato biometrico rappresenta un atto materiale e non una dichiarazione di volontà, risulta certamente esclusa l'applicabilità del diritto al silenzio. Tuttavia, tali operazioni consistono, di volta in volta, in forme di cooperazione o forzata (l'apposizione coattiva del dito su un sensore), o quantomeno surrettizia (il passaggio dello *smartphone* davanti al viso, per lo sblocco) che obbligano l'individuo a compiere o a subire un'azione che, di fatto, determina l'accesso a informazioni potenzialmente auto indizianti. In ragione di ciò, pare doveroso chiedersi se, fuori dal contesto applicativo del diritto al silenzio, non sia invece opportuno recuperare la più ampia garanzia del *privilege against self-incrimination.*

A questo proposito, merita particolare attenzione una pronuncia di qualche anno fa della Corte Suprema olandese, la quale ha stabilito che la sottoposizione a riconoscimento biometrico per sbloccare uno *smartphone*, mediante l'apposizione forzata dell'impronta digitale dell'indagato, non integri una violazione del *nemo tenetur se detegere* [45]. Nello specifico, il caso

---

[44] Sul punto v. https://www.lastampa.it/tecnologia/news/2019/01/16/news/la-polizia-non-puo-costringere-a-sbloccare-un-iphone-protetto-da-faceid-o-touchid-1.33671588; https:// www.forbes.com/sites/thomasbrewster/2016/10/16/doj-demands-mass-fingerprint-seizure-to-open-iphones/; https://appleinsider.com/articles/16/05/02/los-angeles-court-orders-woman-to-unlock-touch-id-equipped-iphone-for-fbi; https://thenextweb.com/news/fbi-uses-faceid-to-unlock-a-suspects-iphone-x-for-the-first-time; https://www.fairtrials.org/news/suspects-privilege-against-self-incrimination-not-violated-when-made-unlock-smartphone.

[45] Cfr. Hoge Raad, 9 febbraio 2021, n. 19/05471, reperibile all'indirizzo https://linkeddata.overheid.nl/front/portal/document-viewer?ext-id=ECLI:NL:HR:2021:202.

riguardava il sequestro probatorio di uno *smartphone* appartenente all'indagato, il quale, in stato di fermo, era stato costretto contro la propria volontà a posizionare il pollice sul lettore biometrico del dispositivo al fine di consentirne l'accesso alle autorità. La questione giuridica centrale concerneva la qualificazione di tale atto come una legittima misura di acquisizione probatoria o, al contrario, come una forma di costrizione idonea a violare il diritto al silenzio e il divieto di auto-incriminazione forzata.

In tale decisione, la Corte olandese ha richiamato l'interpretazione della Corte di Strasburgo che considera l'acquisizione di «*material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect*» non incompatibile con il principio del *nemo tenetur se detegere*, in quanto i mezzi intrusivi impiegati dalle autorità riguardano materiale che non rientra nell'area protetta dal diritto al silenzio[46].

La Corte Suprema olandese, dunque, nel pronunciarsi sulla legittimità dell'accesso forzato a un dispositivo digitale mediante l'impronta biometrica del suo proprietario, ha ritenuto che il dato biometrico, essendo preesistente e indipendente dalla volontà dell'indagato di rilasciarlo, non rientri nella sfera protetta dal principio del *nemo tenetur*. Secondo questa impostazione, l'apposizione coattiva del pollice sul lettore del dispositivo non configurerebbe una violazione delle garanzie difensive, poiché non richiederebbe alcuna forma di cooperazione attiva da parte del soggetto coinvolto. L'impronta digitale sarebbe dunque assimilata a un dato fisico oggettivo, acquisibile al pari di altre evidenze materiali, quali campioni biologici o impronte papillari rilevate nel contesto delle ordinarie attività investigative.

Ulteriore elemento di rilievo nella decisione dei giudici olandesi riguarda la specifica tecnologia impiegata nel telefono sequestrato. In particolare, è stato sottolineato che, al momento della procedura, il livello di sicurezza avanzato del sistema biometrico impediva l'adozione di metodi alternativi di accesso, anche attraverso l'utilizzo degli strumenti tecnici messi a disposizione dal *Netherlands Forensic Institute* (NFI). Tale circostanza è stata ritenuta un fattore dirimente nel giustificare il ricorso alla coercizione fisica per ottenere l'accesso al contenuto del dispositivo, ponendo l'accento sull'inevitabilità della misura per il raggiungimento delle finalità investigative.

In questa prospettiva, i giudici nazionali hanno cercato di operare un

---

[46] C. eur., Grande Camera, 17 dicembre 1996, *Saunders v. The United Kingdom*, 43/1994/490/672, § 69 e *Funke v. France*, 25 febbraio 1993, App. no. 10828/84.

bilanciamento tra due esigenze contrapposte: da un lato, la necessità di accedere ai dati digitali archiviati nel dispositivo, al fine di ricostruire il fatto di reato e raccogliere elementi probatori utili al procedimento; dall'altro, il rispetto del diritto dell'indagato a non essere costretto a contribuire attivamente alla propria auto-incriminazione. Nel tentativo di giustificare tale compromesso, il giudice olandese ha richiamato la giurisprudenza della Corte di Strasburgo, evidenziando che, per valutare la compatibilità di una misura coercitiva con l'art. 6 Conv. eur. dir. uomo, occorre considerare non solo la natura del materiale oggetto di indagine, ma anche «*the nature and degree of the compulsion, the existence of any relevant safeguards in the procedures and the use to which any material so obtained is put*»[47]. In altre parole, il giudizio sulla legittimità della coercizione deve tenere conto dell'intensità della costrizione esercitata, della presenza di garanzie procedurali adeguate e delle finalità per cui i dati acquisiti verranno impiegati nel procedimento.

Da tale impostazione discenderebbe la conclusione secondo cui l'atto di apporre forzatamente il pollice dell'indagato sul sensore biometrico del dispositivo, configurandosi come una forma di coercizione di grado minimo e incidendo in modo limitato sull'integrità fisica del sospettato, non sarebbe idoneo a determinare una violazione dell'art. 6 della Convenzione. Ne deriverebbe, dunque, una distinzione tra forme di coercizione ritenute accettabili nel quadro delle attività investigative e quelle che, invece, supererebbero il limite della protezione convenzionale, imponendo un criterio di valutazione fondato sul grado di intensità dell'intrusione.

L'orientamento interpretativo adottato solleva diversi interrogativi sotto il profilo della tutela delle garanzie fondamentali dell'indagato. L'evoluzione tecnologica impone un costante processo di rivalutazione e reinterpretazione dei principi posti a presidio dell'indagato, in particolare del *nemo tenetur se detegere,* la cui applicazione non può rimanere ancorata a criteri esegetici elaborati in contesti tecnologicamente meno avanzati[48]. Diviene quindi necessario interrogarsi sulla perdurante idoneità di parametri quali «*the nature and degree of the compulsion*» o il requisito dell'esistenza autonoma del materiale oggetto di acquisizione forzata, al fine di verificare se essi

---

[47] Cfr. *Tirado Ortiz e Lozano Martin c. Spagna* 15 giugno 1999, App. no. 43486/98 e *Jalloh c. Germania*, 11 luglio 2006, App. no. 54810/00, cit.

[48] Cfr. W. ZONTEK, *Biometric Encryption of Smart Devices and the Prohibition against Self-incrimination in Criminal Procedure. Old Guarantees in the New World*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 32, 2024, p. 173.

rappresentino ancora uno strumento adeguato per garantire la protezione dell'indagato nel mutato contesto digitale.

L'atto di consegnare alle autorità inquirenti la propria impronta digitale o, in misura ancor più agevole, la propria immagine facciale, sebbene comporti una forma di intrusione nella sfera fisica dell'individuo apparentemente minima e impercettibile, implica in realtà un coinvolgimento attivo nel procedimento [49]. L'indagato, attraverso una minima coercizione o un'esposizione surrettizia, finisce per fornire un contributo sostanziale all'accertamento dei fatti, trasformando il proprio corpo in uno strumento investigativo al servizio dell'autorità. Infatti, anche quando l'acquisizione dell'impronta digitale o del riconoscimento facciale avvenga senza la partecipazione volontaria dell'indagato, il risultato dell'azione coercitiva coincide con l'estrazione di un'informazione riservata [50]. In questo senso, il riconoscimento facciale utilizzato per accedere al contenuto di un dispositivo

[49] In questo senso cfr. J. CZERNIAWSKI-C. BOYACK, *Reviewing the Privacy Implications of Law Enforcement Access to and Use of Digital Data*, in *5 Utah J. Crim. L.* 73 (2021) e W. ZONTEK, *Biometric Encryption of Smart Devices and the Prohibition against Self-incrimination in Criminal Procedure. Old Guarantees in the New World*, cit., p. 174.

[50] In ragione della natura particolarmente sensibile delle informazioni custodite all'interno dei dispositivi digitali – quali *smartphone, tablet* e computer portatili – l'accesso a tali strumenti da parte dell'Autorità giudiziaria implica inevitabilmente un'ingerenza significativa nella sfera privata dell'individuo. I dati contenuti, infatti, possono spaziare da messaggi multimediali a conversazioni personali, dalla cronologia di navigazione a informazioni geolocalizzate, offrendo così un quadro dettagliato e pervasivo della vita privata, relazionale e comportamentale del soggetto. Peraltro, l'interpretazione giurisprudenziale, sia nazionale che sovranazionale (cfr. *ex multis* CGUE, Grande Sez., 4 ottobre 2024, C-548/21, Cass. pen., sez. II, 23 marzo 2023, n. 17604, in *CED Cass.*, n. 284393, Cass. pen., sez. III, 4 luglio 2024, n. 36776, in *CED Cass.*, n. 286923), riconosce il principio per cui non può essere imposto all'indagato alcun obbligo di collaborazione attiva volto a facilitare l'accesso a questi dati. In particolare, il soggetto sottoposto a indagini non può essere sanzionato per il rifiuto di rendere disponibili strumenti o codici di accesso ai dispositivi personali. In tale direzione si colloca in particolare la pronuncia della Corte di cassazione, Cass. pen., sez. II, 23 marzo 2023, n. 17604, in *CED Cass.*, n. 284393, che ha sottolineato che «la mancata collaborazione dell'indagato nel fornire le chiavi di accesso è un comportamento sicuramente inquadrabile come esercizio di una facoltà difensiva, che trova supporto nella ampia tutela che il codice di rito fornisce all'accusato, riconoscendogli, tra l'altro, il "diritto al silenzio"». Il rifiuto di cooperazione, in assenza di un obbligo giuridico positivo, non può pertanto determinare effetti pregiudizievoli sul piano processuale, né può essere considerato alla stregua di una condotta illecita o di ostacolo alle indagini. L'orientamento consolidato impone al legislatore e agli operatori del diritto una riflessione più ampia sulla necessità di bilanciare l'efficacia investigativa con il rispetto delle libertà fondamentali, evitando derive che, in nome della sicurezza o della celerità procedimentale, compromettano i valori di uno Stato di diritto.

digitale senza il consenso dell'indagato, o addirittura in aperto contrasto con la sua volontà, costituisce un atto che, per le sue implicazioni, non può essere considerato estraneo alla protezione offerta dal principio in parola.

La giurisprudenza non può trascurare il fatto che le nuove tecnologie modificano radicalmente i contorni del concetto di libertà personale e autodeterminazione, rendendo necessaria una continua ridefinizione dei confini tra l'autonomia individuale e i poteri coercitivi dello Stato [51]. In un simile quadro, la riflessione giuridica deve necessariamente tenere conto delle attuali soluzioni tecnologiche, al fine di garantire un bilanciamento tra le esigenze di rapidità e di efficienza dell'accertamento investigativo e il rispetto della libertà di autodeterminazione dell'individuo. L'esercizio di questa facoltà non può essere ridotto a un aspetto secondario del procedimento, ma deve rimanere una garanzia irrinunciabile, a tutela dell'equità del processo e della persona sottoposta a indagine [52].

4. *Il trattamento del dato biometrico digitalizzato nel rispetto del diritto alla riservatezza*

La rivoluzione digitale e la conseguente "datificazione" delle nostre vite costantemente mediate e captate da dispositivi digitali ha creato nuove configurazioni e modalità di esercizio dei diritti fondamentali sorti in epoca predigitale e ha reso necessaria una nuova teorizzazione soprattutto del diritto alla protezione dei dati personali e della tutela della riservatezza [53]. Quest'ultima, da ricondurre a livello sovranazionale agli artt. 8 Conv. eur. dir. uomo, 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (CDFUE) [54],

---

[51] Cfr. S. RODOTÀ, *Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, su https://www.privacy.it/archivio/rodo20040916.html; S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997, p. 165; S. RODOTÀ, *Trasformazioni del corpo*, in *Pol. dir.*, 2006, p. 3 ss.

[52] Cfr. V. PATANÉ, *Il diritto al silenzio dell'imputato*, Giappichelli, Torino, 2006, p. 80.

[53] Sul tema cfr. T. ALESCI, *Il corpo umano fonte di prova*, cit., p. 26 ss.; L. LUPARIA, *Diritto alla privacy*, in L. KALB (a cura di), *Diritti della persona e nuove sfide del processo penale*, Giuffrè, Milano, 2019, p. 97; G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 68 ss. e M. TORRE, *Privacy e indagini penali*, Giuffrè, Milano, 2020, p. 3 ss.

[54] Nell'art. 8 Conv. eur. dir. uomo è cristallizzato il diritto al rispetto della vita privata e familiare. Esso può subire ingerenze da parte dello Stato solo se «tale ingerenza sia prevista

non trova invece un'espressa disciplina nella Costituzione e, per questa ragione, è stata collocata, non sempre unanimemente[55], tra i "diritti inviolabili dell'uomo", garantiti dall'art. 2 Cost.[56], conferendole originariamente un contenuto essenzialmente negativo, come pretesa di escludere altri dalla conoscenza di vicende strettamente personali e familiari[57].

La riservatezza si caratterizza per una dinamicità che rende complessa la chiara e definitiva delimitazione dei suoi confini. In ragione della sua progressiva capacità espansiva, tale diritto si avvicina e si intreccia inestricabilmente con il più ampio e sfaccettato concetto di "privacy"[58], in una relazione che ne sottolinea la reciproca interdipendenza e complessità. Tale garanzia ha assunto nel tempo la qualifica di precondizione per l'esercizio di molteplici diritti, dalla libertà di movimento a quella di riunione,

---

dalla legge» e sia «necessaria in una società democratica». Cfr. l'art. 16 TFUE (ove si tutela il diritto di ogni persona alla protezione dei dati di carattere personale che la riguardano) e, con riferimento alla Carta dei diritti fondamentali dell'Unione europea (da qui in avanti CDFUE), cfr. l'art. 7 (diritto al rispetto della vita privata e della vita familiare) e l'art. 8 (protezione dei dati di carattere personale).

[55] Per una ricostruzione cfr. S. CARNEVALE, *Autodeterminazione informativa e processo penale*, in D. NEGRI (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Aracne, Roma, 2007, p. 9 ss.; S. RODOTÀ, *Tecnologie e diritti*, il Mulino, Bologna, 1995, p. 22 ss. Per un approfondimento sulle iniziali diverse interpretazioni dottrinarie v. S. SCAGLIARINI, *La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio*, Aracne, Roma, 2013, p. 43 ss.; M. TORRE, *Privacy e indagini penali*, Giuffrè, Milano, 2020, p. 7 ss.; M. BONETTI, *Riservatezza e processo penale*, Giuffrè, Milano, 2003, p. 9 ss.; A. BARBERA, *Commento all'art. 2 Cost.*, in G. BRANCA, *Commentario alla Costituzione. Principi fondamentali*, Zanichelli, Bologna, 1975, p. 80 ss.

[56] Secondo S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit.dir. priv.*, 4, 1997, p. 606, la tutela alla "privacy" andrebbe ricondotta nell'alveo dell'art. 2 Cost. e dell'art. 3 Cost. ove si menziona l'eguaglianza e la "dignità sociale". Secondo G. DI PAOLO, *"Tecnologie del controllo" e prova penale*, cit., p. 240, 241 e 242, «oltre alla clausola generale dell'art. 3 Cost. potrebbe anzitutto soccorrere l'art. 13 Cost. (…) disposizione (…) interpretata estensivamente, nel senso di ricomprendere all'interno del concetto di libertà personale anche la dignità dell'individuo», ovvero, secondo l'Autrice «si potrebbe sostenere (…) che il diritto alla riservatezza sia desumibile in via sistematica dalla tutela di una serie di diritti già esplicitamente riconosciuti dalla Carta fondamentale, e precisamente dagli artt. 13, 14, 15, 21 Cost.».

[57] Cfr. O. POLLICINO, sub *Art. 8*, in R. MASTROIANNI-O. POLLICINO-S. ALLEGREZZA-F. PAPPALARDO-O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, Milano, 2017, p. 135 ss. Per una ricostruzione storica cfr. M. TORRE, *Privacy e indagini penali*, cit., p. 7 ss.

[58] Per un approfondimento sulle diverse tipologie di privacy, cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 72 ss.

sino alla libertà di espressione, per citare solo i più rilevanti.

Per questa ragione, la tecnologia di riconoscimento facciale è in grado di incidere su una molteplicità di estrinsecazioni del concetto di privacy, ben più ricche di quelle ipotizzate nel "*right to be let alone*" del XIX secolo. Si considerino, per esempio, le potenziali violazioni della cd. "privacy fisica" riferita al corpo [59], ovvero di quella "comportamentale", con riguardo alle ingerenze sulla libertà di riunione [60]. Oppure, si pensi alle applicazioni della tecnologia di riconoscimento facciale finalizzate alla categorizzazione dei dati attraverso l'analisi delle caratteristiche facciali, aventi l'obiettivo di inferire lo stato emotivo, i tratti distintivi della personalità, le inclinazioni politiche o le preferenze sessuali.

A fronte della sempre maggiore capacità intrusiva digitale, la protezione della riservatezza e della privacy si sono saldate progressivamente nell'ulteriore dimensione della tutela dei dati personali [61]. Si è passati dunque da un approccio alla riservatezza intesa con un'accezione "negativa", volta ad escludere le altrui interferenze dai propri fatti e opinioni, alla consacrazione di un diritto "positivo" a mantenere un controllo sull'insieme dei dati riferibili alla persona.

A questo proposito, il quadro normativo si articola tanto a livello internazionale ed europeo [62], quanto nella disciplina di recepimento interno [63].

---

[59] Nel contesto nordamericano, il concetto di privacy ha progressivamente assunto una funzione assiologicamente centrale, sino a sovrapporsi, in termini sostanziali, al nucleo essenziale del concetto di libertà individuale. La giurisprudenza statunitense – a partire dalle pronunce della Corte Suprema – ha infatti riconosciuto alla privacy una portata espansiva, includendovi ambiti esistenziali particolarmente sensibili e caratterizzati da una forte componente di autodeterminazione personale. Essa è divenuta così il fondamento giuridico per la tutela di scelte intime e identitarie, quali quelle relative alla pianificazione familiare e alla contraccezione (*Griswold v. Connecticut*, 1965), all'interruzione volontaria della gravidanza (*Roe v. Wade*, 1973), alle decisioni concernenti il fine vita (*Cruzan v. Director*, 1990), nonché alla libertà di contrarre matrimonio indipendentemente dall'orientamento sessuale (*Obergefell v. Hodges*, 2015). Cfr. S. SCAGLIARINI, *La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio*, Aracne, Roma, 2013, p. 29 ss.

[60] G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 73 ss.

[61] G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 74 ss.

[62] Cfr. le *Guidelines for the Regulation of Computerized Personal Data Files*" adottate dall'Assemblea generale delle NU con risoluzione 45/95 del 14 dicembre 1990, o la risoluzione 34/7 su "*The right to privacy in the digital age*" (A/HRC/RES/34/7) del 23 marzo 2017; le "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*" adottate dall'OCSE nel 1980, approvate in una nuova versione nel 2013; la "Risoluzione di Madrid" adottata nel 2009 dalla *International Conference of Data Protection and Privacy Commissioners.*

[63] Cfr. il d.lgs. n. 101/2018 per l'adeguamento della normativa nazionale alle disposizioni del

Nell'ambito del Consiglio d'Europa, un primo punto di riferimento può essere individuato nella "Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale" (cd. Convenzione 108) del 1981, ratificata in Italia con legge 21 febbraio 1989, n. 98 [64], e con la conseguente Raccomandazione n. R(87) 15 del Comitato dei Ministri per "regolamentare l'utilizzo dei dati a carattere personale nel settore della polizia", del 17 settembre 1987.

Accanto alla normativa formulata dal Consiglio d'Europa, si collocano le disposizioni introdotte dalle istituzioni europee in attuazione degli artt. 8 TUE e 16 TFUE. Il quadro normativo vigente è costituito dal cd. "pacchetto protezione dati", adottato nel maggio 2016, a cui si riconosce pacificamente il merito di aver reso per la prima volta uniforme, nello spazio eurounitario, la normativa riguardante la protezione dei dati personali. Le disposizioni contemplano il regolamento (UE) 2016/679 "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (cd. GDPR) [65], e la direttiva 2016/680/UE del 27 aprile 2016, "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" (cd. LED) [66].

Il campo applicativo del regolamento risulta piuttosto ampio: è lo stesso

---

regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati); d.lgs. n. 51/2018 per l'attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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; d.P.R. 15 gennaio 2018, n. 15 recante il regolamento a norma dell'art. 57 del d.lgs. 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia.

[64] La Convenzione 108 è stata successivamente rinnovata profondamente dal protocollo di modifica (cd. Convenzione 108+). Per un approfondimento cfr. G. GREENLEAF, *Renewing Convention 108: The CoÈs 'GDPR Lite' Initiatives*, 142 *Privacy Laws & Business International Report*, 14-17 agosto 2016. Cfr. il capitolo II, § 2.

[65] Da qui in avanti GDPR.

[66] Da qui in avanti LED.

art. 2 a esplicitarne l'ambito di operatività, escludendo il trattamento di dati «effettuato dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse» (art. 2, par. 2, lett. d), che è invece oggetto della direttiva 2016/680/UE [67], recepita nel nostro ordinamento con il d.lgs. n. 51/2018 [68].

La direttiva costituisce dunque una *lex specialis* rispetto al regolamento, ponendosi come parte di una «complementarietà integrata» [69]: la disciplina ivi contenuta racchiude un inevitabile bilanciamento tra l'interesse del singolo alla tutela dei dati personali e le esigenze di sicurezza sociale e, più in generale, di natura pubblicistica, connesse alla tutela dell'ordine pubblico e alla cooperazione tra le diverse autorità di pubblica sicurezza [70].

Con riferimento alle specifiche disposizioni previste a tutela del dato biometrico, mentre l'art. 9 GDPR vieta, in linea di principio, il trattamento di

---

[67] La direttiva quindi non si applica ai soggetti che effettuano un trattamento di dati per finalità previste dal regolamento (UE) 2016/679. Le disposizioni ivi contenute si applicano a tutti i trattamenti di dati personali effettuati per finalità in essa previste, a prescindere dal fatto che siano non automatizzati, parzialmente automatizzati o interamente automatizzati. Il considerando 11 LED specifica la *ratio* della direttiva, ossia l'introduzione di norme specifiche relative 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 (incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica), nel rispetto della natura specifica di tali attività.

[68] Il d.lgs. 18 maggio 2018, n. 51, pubblicato in *G.U.* 24 maggio 2018, n. 119 riproduce integralmente il contenuto della direttiva 2016/680/UE. Cfr. L. PULITO, *Il trattamento dei dati personali in ambito penale e l'uso del passenger name record per contrastare il terrorismo e altri gravi reati*, in *Proc. pen. giust.*, 2018, p. 1141; A. RICCI, *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati. Riflessioni sul d.lgs. 18 maggio 2018, n. 51, di attuazione della dir. 2016/680/UE*, in *Nuove leggi civ. comm.*, 42(39), 2019, p. 565-598.

[69] Cfr. B. GALGANI, *Giudizio penale, habeas data e garanzie fondamentali*, cit., p. 3.

[70] Cfr. *ex multis* B. GALGANI, *Giudizio penale, habeas data e garanzie fondamentali*, in *Arch. pen.*, 1/2019, p. 3 ss.; A. RICCI, *Il trattamento dei dati personali per finalità di prevenzione, indagine, accertamento e perseguimento dei reati. Riflessioni sul d.lgs. 18 maggio 2018, n. 51, di attuazione della dir. 2016/680/UE*, cit., p. 572; P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, in S. SICA-V. D'ANTONIO-G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Giuffrè, Milano, 2016, p. 313 ss.; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 87 ss.; A. FONSI, *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time*, in *Riv. pen. dir. e proc.*, 13 maggio 2021, p. 4.

tali informazioni [71], l'art. 10 della direttiva, stabilisce che sia autorizzato «solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato», qualora sia presente una previsione normativa nel diritto dell'Unione o dello Stato membro (lett. a), per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica (lett. b), o se il suddetto trattamento riguardi dati resi manifestamente pubblici dall'interessato (lett. c). La disposizione deve essere interpretata in combinato disposto con l'art. 52, par. 1, CDFUE, secondo cui le eventuali limitazioni all'esercizio di un diritto fondamentale devono essere «previste dalla legge» [72], intendendosi con tale locuzione la necessaria presenza di una base giuridica che autorizzi la limitazione in modo chiaro e preciso [73], che disciplini «la portata e l'applicazione» della misura limitativa e che imponga «requisiti minimi», in modo che le persone i cui dati sono trattati dispongano di «garanzie sufficienti» per proteggere efficacemente i propri dati contro il rischio di abusi, nonché contro eventuali accessi e usi illeciti [74]. Analogamente, l'art. 8, par. 2 della Conv. eur. dir. uomo richiede che le limitazioni al diritto al rispetto della vita privata siano "previste dalla legge".

La Corte EDU, in più occasioni, ha specificato i requisiti di "accessibilità" e "prevedibilità" normativa, stabilendo che la legislazione nazionale deve essere sufficientemente chiara da consentire alle persone di agire consapevolmente in conformità alla legge e delimitare la portata della discrezionalità delle decisioni delle autorità pubbliche [75].

---

[71] L'art. 9, par. 2, stabilisce che il trattamento è consentito solo se l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche per assolvere obblighi o esercitare diritti in ambito lavorativo e previdenziale (b); qualora sia necessario tutelare un interesse vitale quando non sia possibile prestare il consenso (c); per il raggiungimento delle finalità di legittime attività di fondazioni, associazioni o altri organismi senza scopo di lucro (d); qualora i dati personali particolari siano resi manifestamente pubblici dall'interessato (e); per lo svolgimento di attività difensive ed investigative (e); per un interesse pubblico rilevante nel settore della sanità pubblica (i); per scopi di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici (j), salvo le possibili deroghe e adeguamenti introdotti dagli Stati membri (art. 89, par. 2).

[72] Cfr. il considerando 35 LED.

[73] Cfr. CGUE 6 ottobre 2020, cause riunite C-245/19, *État luxembourgeois* c. B) e C-246/19, *État luxembourgeois* c. B, C, D, F.C.).

[74] CGUE 8 aprile 2014, *Digital Rights Ireland and Others*, Joined Cases C-293/12 and C-594/12, § 54; CGUE 16 luglio 2016, *Data Protection Commissioner v Facebook Ireland Limited and Maxmilian Schrems*, Case C-311/18, § 176.

[75] C. eur. 28 novembre 2011, *Shimovolos v. Russia*, n. 30194/09, § 68, *Malone c. Regno*

A questo proposito, i giudici di Strasburgo hanno posto particolare attenzione al concetto di "qualità delle norme": la legge interna deve indicare la natura, la portata e la durata delle misure limitative dei diritti fondamentali, la loro base giuridica, le autorità competenti ad autorizzare tali misure e la tipologia di rimedi a disposizione. Sul legislatore nazionale grava dunque l'obbligo di introdurre una normativa interna disciplinante l'acquisizione e la conservazione dei dati biometrici e genetici, che non sia affetta da profili di ambiguità e incertezza.

Già a partire da questi primi arresti giurisprudenziali emerge evidentemente l'importanza attribuita non tanto alla presenza formale dell'atto legislativo, quanto piuttosto alla "sostanza" e alla "qualità" delle norme, valutate in relazione diretta alla tecnologia considerata [76]. Coerentemente con tale approccio, l'art. 6 LED prevede la necessità di evitare che sia imposta indistintamente un'ingerenza della medesima intensità nei confronti dei soggetti indicati nell'elenco previsto dalla stessa disposizione, suggerendo agli Stati membri di realizzare, «nei limiti del possibile», una diversificazione chiara tra le varie categorie di interessati (per esempio, tra indagato e persona offesa) [77]. La logica sottesa a questa diversificazione mira ad assicurare un livello di protezione più elevato a favore dei titolari di dati che non rivestono la posizione di destinatari dell'addebito [78]. Per questi ultimi, l'art. 6 richiede, in termini piuttosto generici, l'esistenza di un compendio indiziario dotato di una certa consistenza, come si desume dal riferimento espresso alle persone per le quali vi siano «fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato». Tale formulazione, sebbene non dettagliatamente articolata, implica che il trattamento dei dati personali non possa basarsi su mere congetture o su presupposti investigativi privi di un minimo supporto probatorio. La vaghezza del dettato normativo lascia tuttavia agli

---

Unito, 2.9.1984, § 67, *Halford c. Regno Unito*, 25 giugno 1997, § 49, *Khan c. Regno Unito*, sez. III, 12 maggio 2000, § 26.

[76] La sussistenza di una legge non è condizione né necessaria, né sufficiente per soddisfare la legalità convenzionale. Cfr. G. PICCIRILLI, *La "riserva di legge". Evoluzioni costituzionali, influenze sovrastatuali*, Giappichelli, Torino, 2019, p. 237 ss.

[77] Con la pronuncia CGUE 28 novembre 2024, V.S., C-80/23, la Corte ha chiarito che spetti al responsabile del trattamento una valutazione in ordine alla praticabilità di una tale distinzione. Inoltre, ad avviso della Corte, se esiste un numero sufficiente di elementi di prova della colpevolezza e vi è fondato motivo di ritenere che la persona abbia commesso il reato, una normativa nazionale che preveda la raccolta coercitiva di dati biometrici e genetici è compatibile con la direttiva.

[78] Cfr. B. GALGANI, *Giudizio penale, habeas data e garanzie fondamentali*, cit., 3.

Stati membri un margine di discrezionalità nell'individuazione dei criteri probatori idonei a giustificare il trattamento, con il rischio che si determini una disomogeneità applicativa a livello nazionale e una conseguente frammentazione della tutela accordata nei diversi ordinamenti giuridici.

Inoltre, la direttiva non si limita a stabilire criteri sostanziali per la legittimità del trattamento dei dati, ma impone anche garanzie procedurali destinate a rafforzare la tutela dell'individuo nei confronti di eventuali abusi o trattamenti illeciti. Nel caso di mancata collaborazione da parte del destinatario del trattamento, la normativa nazionale che consente la raccolta deve garantire, altresì, il diritto ad una tutela giurisdizionale effettiva, ai sensi dell'art. 47 della Carta di Nizza. L'art. 54 della direttiva impone infatti agli Stati membri di disporre che, «fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'art. 52, l'interessato abbia il diritto a un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode ai sensi delle disposizioni adottate a norma della […] direttiva siano stati violati».

L'insieme di queste norme evidenzia il delicato bilanciamento perseguito dal legislatore europeo tra le esigenze di sicurezza pubblica e la necessità di tutelare i diritti fondamentali dell'individuo. Già a partire da questo inquadramento sistematico, riecheggia immediatamente l'importanza fondamentale rivestita, in questo specifico settore, dal principio di *proporzionalità* tra mezzi e finalità del trattamento [79], la cui valutazione dev'essere eseguita caso per caso, tenendo conto della limitazione dei diritti, dello scopo e del contesto di impiego [80]. Infatti, l'art. 52 CDFUE non si limita solamente a stabilire l'esigenza di una legge, ma fa riferimento anche alla necessità che venga rispettato il principio di proporzionalità, da intendersi come strumento di ragionamento giudiziario che consente alle Corti di vincolare l'intervento dello Stato a diritti e valori costituzionali [81]. Il rispetto di questo principio è divenuto col tempo metro e condizione per valutare la legittimità delle misure limitative dei diritti fondamentali: a

[79] Cfr. gli artt. 5, 8, 10 LED e il considerando 26 LED.

[80] In questo senso, occorre tenere bene distinte le finalità preventive e investigative nell'utilizzo di questi *tools* da parte della autorità di *law enforcement.*

[81] Cfr. G. MOBILIO, *L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?*, in E. DI CARPEGNA BRIVIO, A. SANCINO (a cura di), *La democrazia della società digitale. Tensioni e opportunità.* Atti del Convegno 3 dicembre 2021. Università di Milano-Bicocca, 2023, p. 14.

questo scopo, la giurisprudenza e la dottrina hanno elaborato un test dalla struttura triadica [82].

Il primo criterio riguarda l'*idoneità* del mezzo, da intendere come l'astratta *adeguatezza* della misura al raggiungimento dell'obiettivo [83]. Il ricorso alla tecnologia di riconoscimento facciale da parte delle forze di polizia può considerarsi *adeguato* agli scopi da essa perseguiti? La Corte di giustizia, con riferimento a questo parametro, ha evidenziato più volte la necessità di definire precisamente gli obiettivi di polizia, richiamando dunque nuovamente l'esigenza di avere regole più stringenti [84]. L'analisi di un *adeguato* ricorso al riconoscimento facciale deve tener conto di una serie di fattori, tra cui l'effettiva capacità dello strumento di raggiungere gli obiettivi prefissati in rapporto al livello di intrusività della misura.

Il secondo requisito riguarda la *necessità*, intesa come "imprescindibilità" del ricorso alla misura per raggiungere gli obiettivi e come esigenza che lo strumento rappresenti il minimo sacrificio necessario per i diritti in gioco. Ne consegue che il trattamento è consentito solo se l'obiettivo non può essere ragionevolmente conseguito in modo altrettanto efficace con mezzi

---

[82] Cfr. A. SANDULLI, voce *Proporzionalità*, in *Dizionario di diritto pubblico*, Giuffrè, Milano, 2006, p. 4644 e 4645; Cfr. C-293/12 e C-594/12, *Digital Rights Ireland*, CJEU, 8 aprile 2014 e C-203/15, *Tele2 Sverige*, CJEU, 21 dicembre 2016.

[83] Cfr. D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, 1/2020, p. 62, «l'idoneità è criterio di razionalità tecnica basato sul nesso di ragionevole strumentalità del mezzo rispetto al fine perseguito. La misura è inidonea se non ha alcun effetto utile oppure rende difficile il raggiungimento dello scopo, mentre anche la semplice possibilità di ottenere il risultato, di facilitarlo in qualche caso, basta a soddisfare il requisito». Secondo F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Wolters Kluwer Cedam, Milano, 2020, p. 124: «devono inoltre sicuramente essere ritenute inidonee al raggiungimento dello scopo le misure che permettono l'acquisizione di informazioni sprovviste di minimi connotati di affidabilità e verificabilità postuma. Il prodotto della ricerca sguarnito di sufficiente efficacia dimostrativa costituisce infatti apporto sostanzialmente inutile alla luce delle finalità cognitive del rito, tanto in dibattimento che durante la fase delle indagini preliminari, non potendo pertanto giustificare alcun sacrificio dei diritti fondamentali». Cfr. CGUE 17 ottobre 2013, C-291/12, *Schwarz*, §§ 45-46, CGUE, C-293/12 e C-594/12 *Digital Rights Ireland*, cit., §§ 46-47.

[84] CGUE 21 dicembre 2016, *Tele2 Sverige AB* (C-203/15) *v. Post– och telestyrelsen e Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*, § 102; CGUE 6 ottobre 2020, *Joined Cases* C-511/18; C-512/18, CGUE, *La Quadrature du Net* (C-511/18 and C-512/18) *v Premier minister and Ordre des barreaux francophones et germanophone v Conseil des ministers*, § 136.

diversi, meno lesivi dei diritti fondamentali delle persone interessate [85]. Per esempio, non potrebbero essere mai considerate necessarie quelle misure investigative atte ad arricchire *ad abundantiam* un compendio ricostruttivo già compiutamente delineato.

Idoneità e necessità sarebbero dunque da intendere in un rapporto non biunivoco: la misura inidonea non potrà mai dirsi necessaria, mentre tra le attività astrattamente idonee occorrerà isolare quelle effettivamente necessarie al perseguimento dell'esigenza che le giustifica.

Infine, il terzo criterio riguarda la *proporzionalità in senso stretto*, da valutare bilanciando il grado di intrusione della misura e l'importanza degli obiettivi da perseguire. Tale valutazione non può risolversi in una mera constatazione astratta della presenza di un interesse pubblico meritevole di tutela, ma deve essere condotta attraverso un'analisi concreta e contestualizzata che tenga conto della specificità dell'impiego della tecnologia e delle sue implicazioni in termini di limitazione dei diritti individuali. Per esempio, considerando le variabili descritte, quando il test della proporzionalità si riferisce al grado di intrusione della tecnologia di riconoscimento facciale, occorre tenere conto del contesto di impiego (es. area geografica interessata), della portata (es. il potenziale numero di persone coinvolte), del grado di intrusività (es. impiego dello strumento in modalità di verifica/autenticazione ovvero identificazione). Parallelamente, si devono considerare gli obiettivi da perseguire (es. controlli di sicurezza alle frontiere o sorveglianza nelle città) e la gravità dei fatti su cui indagare (es. terrorismo) [86]. Il ricorso agli strumenti di riconoscimento facciale può essere giustificato più facilmente in situazioni che presentano un elevato grado di rischio per la sicurezza pubblica, mentre l'impiego della tecnologia per scopi, per esempio, di natura meramente amministrativa – come la gestione della viabilità urbana o la prevenzione di reati minori – risulta assai più critico, in quanto il sacrificio del diritto individuale non appare giustificato da una corrispondente necessità pubblica imperativa.

[85] Da ultimo cfr. CGUE 28 novembre 2024, in causa C-80/23.

[86] *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, 2022.

4.1. *Un'ipotesi specifica di trattamento: il processo decisionale automatizzato*

L'importanza di prevedere adeguate garanzie risulta ancora più cruciale quando i dati personali sono oggetto di un *trattamento decisionale automatizzato* [87].

La correttezza del *processo decisionale automatizzato* [88] – entro la cui categoria potrebbe essere ricondotto il procedimento algoritmico alla base dei sistemi di riconoscimento facciale [89], e che può portare ad assumere una decisione in grado di incidere «significativamente sull'interessato», con «effetti giuridici negativi» – deve essere garantita in tutti i settori nei quali vengono effettuate scelte che interessano i diritti delle persone [90]. Si pensi, ad esempio,

---

[87] CGUE C-311/18, *Data Protection Commissioner*, cit., p. 176. Cfr. J. SAJFERT-T. QUINTEL, *Data Protection Directive (EU) 2016/680 for police and criminal justice authorities*, su https://ssrn.com/abstract=3285873.

[88] Artt. 22 GDPR e 11 LED. La nozione di "processo decisionale automatizzato" comprende non solo provvedimenti giurisdizionali conclusivi di un procedimento, ma anche valutazioni sulle prove, basate su elaborazioni algoritmiche di dati e produttive di effetti giuridici, le quali non prevedono l'intervento umano, sebbene la decisione sia da imputarsi formalmente all'uomo. In altre parole, si applica a situazioni in cui la decisione viene presa senza il coinvolgimento dell'uomo e, quindi, deve essere garantita una supervisione sulla decisione per non incorrere in pregiudizi o risultati discriminatori. La Corte di giustizia si è pronunciata sul tema, tratteggiando i confini della nozione di "decisione", conferendole una portata assai ampia. In particolare, entro tale categoria si riconduce sia una "misura", sia una "valutazione", purché concerna aspetti di carattere personale e vi sia un'incidenza, seppur minima, sulla sfera personale degli interessati. Cfr. CGUE 7 dicembre 2023, C-634/21, *SCHUFA Holding AG*, ECLI:EU:C:2023:957, § 45 ss. Per un approfondimento cfr. A. AZA, *Scores as Decisions? Article 22 GDPR and the judgement of the CJEU in SCHUFA Holding (Scoring) in the Labour Context*, in *Industrial Law Journal*, 2024; F. PALMIOTTO, *When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis*, in *German Law Journal*, 2024, p. 1-27.

[89] «(…) *a score is more than a preliminary measure in the wider process of decision-making, capable of producing appreciable consequences*», A. AZA, *Scores as Decisions? Article 22 GDPR and the judgement of the CJEU in SCHUFA Holding (Scoring) in the Labour Context*, in *Industrial Law Journal*, 2024, riguardo a quanto sostenuto CGUE, C-634/21, *SCHUFA Holding AG, Preliminary Request*, 15 ottobre 2021, § 25, «*it is ultimately the score […] that actually decides whether and how the third-party controller enters into a contract with the data subject*».

[90] Cfr. F. DONATI, *Intelligenza artificiale e giustizia*, cit., p. 425; J. SAJFERT-T. QUINTEL, *Data Protection Directive (EU) 2016/680 for police and criminal justice authorities*, in M. COLE-F. BOEHM (eds.), *GDPR Commentary*, 2018, p. 10; L.A. BYGRAVE, *Article 22 Automated individual decision-making including profiling*, in C. KUNER *et al.* (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020; R. BINNS, M.

all'impiego di strumenti automatizzati che permettono o impediscono l'accesso ad un determinato servizio, come il trasporto aeroportuale, o che possono precludere l'ammissione a certe agevolazioni o sussidi.

In questi casi, la normativa europea stabilisce che l'interessato abbia il diritto, non solo di essere informato circa l'esistenza di un procedimento di tale natura che tratti i suoi dati, ma anche di ottenere l'intervento di un essere umano qualora possano derivarne effetti pregiudizievoli [91]. L'obiettivo è quello di assicurare la partecipazione di un soggetto umano, con gradi di intensità diversa (c.d. *human-in-the-loop, human-on-the-loop, human-in-command* [92]), nell'assunzione di decisioni riguardanti la vita di altri esseri umani, assicurando un meccanismo di supervisione umana per impedire eventuali violazioni o danni provocati dal cattivo funzionamento delle macchine [93].

VEALE, *Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR*, in *International Data Privacy Law*, fasc. II(4), 2021, p. 319-322; G. MALGIERI-G. COMANDÈ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, fasc. 7(2), 2017.

[91] Cfr. C. CAVACEPPI, *L'intelligenza artificiale applicata al diritto penale*, in G. TADDEI ELMI-A. CONTALDO (a cura di), *Intelligenza artificiale. Algoritmi giuridici Ius condendum o "fantadiritto"?*, Pacini, Pisa, 2020, p. 128; F. PIZZETTI, *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018, p. 30.

[92] "*Human-in-the-loop*" si riferisce all'intervento umano in ogni ciclo decisionale del sistema. "*Human-on-the-loop*" si riferisce alla possibilità che l'intervento umano avvenga durante il *design* del sistema e come monitoraggio durante il suo funzionamento. "*Human-in command*" si riferisce invece alla possibilità di vigilare sull'attività complessiva di un sistema di IA (compreso il più ampio impatto economico, sociale, etico e legale) e alla capacità di decidere come e quando usare il sistema in una situazione particolare. Cfr. *Communication "Building Trust in Human-Centric Artificial Intelligence*", COM(2019) 168 final, 8 aprile 2019, p. 4. Un approccio rigoroso alla questione appena segnalata giunge dalla giurisprudenza amministrativa che riconosce: «alla persona il diritto di non essere sottoposta a decisioni automatizzate prive di un coinvolgimento umano [...]. Quindi occorre sempre l'individuazione di un centro di imputazione e di responsabilità, che sia in grado di verificare la legittimità e la logicità della decisione dettata dall'algoritmo». A tale garanzia, il giudice amministrativo affianca i seguenti principi generali fondamentali in favore del soggetto interessato dal trattamento: principio di conoscibilità, in base al quale «ognuno ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino ed in questo caso a ricevere informazioni significative sulla logica utilizzata»; principio di non esclusività della decisione algoritmica (cd. *human in the loop*): nel caso in cui vi sia una decisione automatizzata, bisogna prevedere un contributo umano capace di controllare, validare ovvero smentire la decisione automatica; principio di non discriminazione algoritmica. Cfr. Cons. Stato, sez. VI, 4 febbraio 2020, n. 881, in *Giur. it.*, 7, 2020, p. 1738.

[93] Cfr. G. FASANO, *L'interpretazione estensiva della nozione di "decisione automatizzata"*

L'intervento umano è una garanzia importante, in grado di ridurre (ma non di eliminare) il rischio che un soggetto subisca l'effetto negativo di un errore valutativo da parte dell'algoritmo [94]. A tal proposito, il Gruppo di lavoro "Articolo 29" [95] ha posto in guardia sulla possibilità di eludere la norma con un atto meramente figurativo, stabilendo che «per aversi un coinvolgimento umano, il titolare del trattamento deve garantire che qualsiasi controllo della decisione sia significativo e non costituisca un semplice gesto simbolico» [96].

La lettura più rigorosa della previsione contenuta nell'art. 11 LED suggerisce che, affinché sia garantito un effettivo intervento umano, una decisione non possa basarsi esclusivamente sull'*output* di un sistema automatizzato [97]. Tale interpretazione troverebbe conferma laddove la stessa normativa sulla protezione dei dati prevede la possibilità di una deroga alla regola generale solo nel caso in cui siano garantite adeguate tutele per i diritti personali e sia comunque assicurato un intervento umano, seppur minimo. Per questo motivo, il dato generato dall'IA non può essere assunto come unico elemento di una decisione, ma deve necessariamente essere verificato attraverso fonti indipendenti, al fine di garantirne l'attendibilità e di evitare il rischio di decisioni basate appunto esclusivamente su processi completamente automatizzati [98].

---

ad opera della Corte di giustizia: una prospettiva più ampia ma ancora fragili tutele per la libertà fondamentali, in *Riv. it. inf. e dir.*, 6(2), 2024, p. 1-15.

[94] Cfr. EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, cit., p. 29.

[95] Cfr. il capitolo II, § 2.

[96] Cfr. *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 2017, p. 23.

[97] Cfr. M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra stati uniti ed europa*, in *Dir. pen. cont. online*, 29 maggio 2019, p. 16.

[98] Anche l'art. 5, par. 3, regolamento (UE) 2024/1689, prescrive che «nessuna decisione che produca effetti giuridici negativi su una persona può essere presa unicamente sulla base dell'*output* del sistema di identificazione biometrica remota "in tempo reale"». In particolare, salvo alcune ipotesi eccezionali (tra le quali rientrano le attività di *law enforcement*, ove tale garanzia risulti sproporzionata), il *deployer* non può compiere azioni o adottare decisioni sulla base dell'identificazione risultante dal sistema, a meno che tale identificazione non sia stata verificata e confermata separatamente da almeno due persone fisiche dotate della necessaria competenza, formazione e autorità (artt. 14, par. 5 e 26, par. 10). Cfr. il capitolo IV, §§ 3.2.2 e 3.2.3.

4.2. *Il perimetro del trattamento tra i principi di limitazione della finalità e di minimizzazione dei dati*

Tornando al principio di proporzionalità, naturalmente, il trattamento dei dati deve rispettare il criterio anche nei suoi corollari della *limitazione della finalità* e di *minimizzazione dei dati*[99]. Con riferimento al primo, ai sensi dell'art. 4, par. 1, lett. b), LED, i dati personali devono essere «raccolti per finalità determinate, esplicite e legittime» e «trattati in modo non incompatibile» con le stesse[100]. La valutazione va eseguita avuto riguardo alla natura dell'obiettivo, che deve essere concreto e coerente con la prevenzione di minacce alla sicurezza pubblica che presentino un certo livello di gravità, la repressione di reati o la protezione contro potenziali violazioni alla luce delle circostanze specifiche in cui il trattamento è effettuato. La finalità di trattare dati biometrici non può essere delineata dagli Stati in termini troppo generici, ma deve essere definita in modo sufficientemente preciso e concreto, anche alla luce del principio di stretta necessità.

La *ratio* della disposizione è quella di rafforzare la libertà di autodeterminazione sui propri dati, esercitando su di essi, quantomeno indirettamente, una forma di controllo, prevenendo la violazione di diritti fondamentali mediante l'utilizzo non dichiarato dei dati o la loro violazione attraverso un accesso illegittimo, e in questo modo promuovendo la fiducia nei destinatari del trattamento.

Per questa ragione, la normativa sui dati personali definisce anche i confini per un riutilizzo legittimo delle immagini per altri scopi (cd. *trattamento secondario*)[101]. In particolare, essa richiede l'autorizzazione da parte del diritto UE o degli Stati e che il trattamento sia «necessario e proporzionato a tale altra finalità»[102]. Gli scopi di polizia non legittimerebbero di per sé il riuso dei dati raccolti: le immagini dei volti catturate durante un'indagine non dovrebbero essere trattate in altre indagini, a meno che tali informazioni siano strettamente necessarie e non siano diversamente reperibili. In questo senso, la disciplina nazionale risulta ambigua, laddove consente la comunicazione dei dati

---

[99] Cfr. CGUE 26 gennaio 2023, in causa C-80/23.

[100] Cfr. l'art. 4, par. 1, lett. b), LED. Il principio costituisce espressione diretta dell'art. 8, parr. 1 e 2, CDFUE ove stabilisce che «ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano» e «tali dati devono essere trattati […] per finalità determinate».

[101] Cfr. l'art. 3, § 4, LED.

[102] Art. 4, § 2, LED.

personali a pubbliche amministrazioni o enti pubblici e a privati quando ciò «risponde all'interesse della persona cui i dati si riferiscono e, comunque, nei singoli casi in cui è necessario per evitare un pericolo grave e imminente alla sicurezza pubblica, o per la salvaguardia della vita e dell'incolumità fisica di un terzo» [103].

In diverse pronunce, la Corte di giustizia ha chiarito che, al fine di procedere ad un legittimo riutilizzo dei dati raccolti, debbano essere necessariamente indicate le «condizioni sostanziali e procedurali», che devono determinare «criteri oggettivi» rigorosamente ristretti e idonei a giustificarne il nuovo impiego rispetto alla finalità perseguita [104]. Nel caso *S. & Marper*, anche la Corte europea dei diritti dell'uomo ha affermato che, nel contesto di utilizzo di dati biometrici, occorre fare riferimento a regole chiare e dettagliate, volte a disciplinare la portata e le modalità di applicazione delle misure, nonché le garanzie minime riguardanti, fra l'altro, la durata, la conservazione, l'utilizzo e le procedure di cancellazione degli stessi, al fine di prevenire il rischio di abusi e riutilizzi arbitrari [105].

Il rispetto di tali condizioni, tuttavia, può sembrare piuttosto complesso per l'impiego di alcuni dati biometrici più facili da captare e potenzialmente di più agevole cessione e circolazione. Le tecnologie di riconoscimento facciale consentono di rielaborare e trattare i dati con modalità e finalità che il titolare del trattamento difficilmente può immaginare al momento della raccolta.

---

[103] Art. 13, comma 3, d.P.R. n. 15/2018. Si definisce "*function creep*" o "scorrimento di funzioni", l'incremento di funzionalità degli scopi iniziali di raccolta dei dati in determinati settori. Per esempio, nel settore della gestione dell'immigrazione, i sistemi informativi EURODAC, SIS, VIS, SID sono stati creati per la raccolta di dati con determinati scopi ma, in presenza di certe circostanze emergenziali, legate per esempio a eventi terroristici, «vivono una sostanziale convergenza verso obiettivi comuni», causando una sostanziale confusione tra gestione dell'immigrazione e contrasto al crimine e al terrorismo. Per un approfondimento sul tema cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, p. 247 ss.; G. CAGGIANO, *L'interoperabilità fra le banche dati dell'Unione sui cittadini degli Stati terzi*, in *Dir., imm. e citt.*, 1, 2020, p. 180; J.P. STUMPF, *The Crimmigration Crisis: Immigrants, Crime, and Sovereign Power*, in *American University Law Review*, 56(2), 2016, p. 367 ss.; E. CELORIA-V. FERRARIS, *Eurodac: dalla gestione delle domande di protezione internazionale al controllo della mobilità*, in *Quad. AISDUE-Riv. quadr.*, fasc. spec. 4, 2024, *Il futuro del diritto e della politica migratoria europea: il Nuovo Patto e oltre*, p. 1-24.

[104] Cfr. *ex multis* CGUE, C-362/14, *Maximillian Schrems*, cit., p. 93; CGUE, parere 1/15 (Accordo PNR UE-Canada), cit., par. 191.

[105] Cfr. C. eur., Grande Camera, 4 dicembre 2008, *S. & Marper c. Regno Unito*, § 99.

L'impiego di alcune tecniche di intelligenza artificiale, poi, applicate nel contesto del trattamento di dati biometrici come l'immagine di un volto, può sfociare in alcune pratiche abusive denominate "*fishing expeditions*", ossia i cd. "rastrellamenti" di immagini, aventi la finalità generica di raccogliere informazioni sulla popolazione per scopi principalmente preventivi, ma il cui utilizzo potrebbe prestarsi anche per finalità repressive [106]. Pertanto, il principio di limitazione della finalità deve trovare applicazione in maniera rigorosa lungo l'intero arco del procedimento penale. Ciò implica che ogni operazione di trattamento di dati personali, e in particolare di dati biometrici, debba risultare funzionalmente e giuridicamente ancorata ad una finalità determinata, esplicita e legittima, conforme agli scopi istruttori o processuali per i quali è stata prevista [107].

Il secondo corollario del principio di proporzionalità concerne la *minimizzazione dei dati:* essi devono essere adeguati, pertinenti e limitati a quanto necessario per le finalità per le quali sono trattati [108]. L'obiettivo è limitare la raccolta dei dati personali, eliminando quelli non essenziali o non conformi allo scopo preposto. Il principio assume, in primo luogo, una particolare rilevanza nel momento in cui il campione biometrico viene sottoposto a conversione in immagine digitale o modello elettronico, poiché la qualità e la quantità delle caratteristiche estratte devono risultare adeguate e funzionali alla comparazione tra *templates* e/o rappresentazioni digitali del tratto biometrico, senza eccedere i parametri strettamente necessari all'utilizzo specificato [109]. Da un lato, i tratti biometrici digitalizzati devono essere dimensionati in modo

---

[106] Cfr. N. STROSSEN, *Post-9/11 Government Surveillance, Suppression and Secrecy*, in A.D. MOORE *et al.* (a cura di), *Privacy, Security and Accountability. Ethics, Law and Policy*, Rowman & Littlefield, New York, 2016, p. 226 ss. Per un'analisi sulla distinzione fra le finalità di "*prevention*" e "*repression*", v. S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, 2020, p. 38 ss. La pratica di "*scraping*" non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso è stata oggetto di uno specifico divieto nel regolamento sull'intelligenza artificiale (UE) 2024/1689 (cfr. il considerando 43 e l'art. 5, par. 1, lett. e). Per un approfondimento sul tema cfr. F.P. LEVANTINO-I.N. REZENDE, *Rischio inaccettabile: usi proibiti*, in O. POLLICINO-F. DONATI-G. FINOCCHIARO-F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, Giuffrè, Milano, 2025, p. 182 ss.

[107] Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., p. 172.

[108] Cfr. l'art. 4, par. 1, lett. c), LED.

[109] Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., p. 174.

coerente rispetto alla tipologia di informazioni contenute, evitando al contempo un accumulo superfluo di dati che potrebbero aumentare il rischio di un trattamento improprio o non conforme alla normativa sulla protezione dei dati personali. Un'eccessiva estrazione di dettagli biometrici potrebbe infatti tradursi in una compressione indebita del diritto alla riservatezza e alla protezione dei dati, alimentando il rischio di una conservazione di informazioni non pertinenti rispetto alla finalità del trattamento. Dall'altro lato, affinché il processo di digitalizzazione del dato biometrico risulti efficace e conforme agli standard di sicurezza, è necessario che le caratteristiche estratte siano sufficientemente dettagliate da consentire una ricostruzione attendibile del dato biometrico originario, permettendo così la comparazione accurata con i dati di riferimento.

V'è da rilevare che il principio in esame potrebbe risultare difficilmente conciliabile con le esigenze dei sistemi di apprendimento automatico, i quali, per garantire livelli elevati di accuratezza e prestazioni, necessitano di un ampio volume di dati da processare e da utilizzare per l'addestramento degli algoritmi [110]. L'antinomia tra questi due elementi emerge con particolare evidenza nell'ambito del riconoscimento biometrico, dove la qualità e l'affidabilità del sistema sono direttamente proporzionali alla quantità di dati impiegati per il *training* dell'algoritmo. Maggiore è il *dataset* a disposizione, più efficace sarà il modello di comparazione, il quale sarà in grado di identificare e affinare *patterns* biometrici complessi, riducendo il margine di errore nelle fasi di verifica e identificazione. Tuttavia, tale logica si pone in potenziale contrasto con il principio di minimizzazione, che impone una raccolta e un trattamento dei dati proporzionati alla finalità perseguita, evitando un'archiviazione indiscriminata di informazioni personali che potrebbero eccedere il necessario. Peraltro, il criterio della minimizzazione si rivela particolarmente efficace per la costruzione delle cd. *watchlist* utili ai fini del riconoscimento *in tempo reale* [111]. L'applicazione del principio in questo contesto implica che tali elenchi debbano essere costruiti secondo criteri rigorosi, escludendo l'inserimento indiscriminato di soggetti privi di un collegamento effettivo e dimostrabile con le finalità di indagine in uno specifico procedimento.

---

[110] Cfr. M. EBERS, *Regulating AI and Robotics: Ethical and Legal Challenges*, in M. EBERS-S. NAVAS NAVARRO (a cura di), *Algorithms and Law*, Cambridge University Press, Cambridge, 2020, p. 64; T. TAULLI, *Artificial Intelligence Basics*, Apress, Berkeley, 2019, p. 36; J. BIEGA-M. FINCK, *Reviving Purpose, Limitation and Data Minimisation in Data-Driven System*, in *Technology and Regulation*, 2021, p. 44-61.

[111] Cfr. il capitolo II, § 4.

Strettamente connesso a questo è il principio della *limitazione della conservazione*, secondo cui i dati personali devono essere registrati e conservati in una modalità che consenta l'identificazione degli interessati per un tempo non superiore al conseguimento delle finalità per cui sono stati trattati [112]. In altre parole, la conservazione dei dati biometrici deve rispettare criteri oggettivi, tenendo sempre in considerazione il rapporto tra i dati da conservare e l'obiettivo da perseguire. Su questo punto, la Corte EDU ha avuto modo di aggiungere che «il carattere generale ed indiscriminato» della conservazione delle impronte digitali, dei campioni di cellule e dei profili di DNA di persone sospettate ma non condannate non assicura il giusto bilanciamento tra i concorrenti interessi pubblici e privati in gioco e, pertanto, «costituisce un'ingerenza sproporzionata nel diritto dei ricorrenti al rispetto della vita privata» [113]. La conservazione dei dati per un periodo indiscriminato di tempo, in assenza di una normativa chiara e dettagliata che specifichi le circostanze che consentono la raccolta, la durata della loro conservazione e l'utilizzo che se ne può fare viola l'art. 8 Conv. eur. dir. uomo.

Più di recente, la Corte di giustizia ha avuto modo di specificare che «anche se il riferimento, nella normativa nazionale, al verificarsi del decesso dell'interessato può costituire un "termine" per la cancellazione dei dati conservati, (…), un siffatto termine può essere considerato "adeguato" solo in circostanze particolari che lo giustifichino debitamente (…)», non essendo «applicabile in modo generale e indifferenziato a qualsiasi persona condannata definitivamente» [114].

Ne consegue che, nel momento in cui sia venuta meno la motivazione che ha giustificato la raccolta dei dati e in assenza di un ulteriore fondamento giuridico, sarà necessario procedere alla cancellazione degli stessi.

In questo contesto, l'innovazione tecnologica potrebbe rappresentare un prezioso strumento di supporto per garantire un equilibrio tra funzionalità ed esigenze di tutela dei diritti fondamentali. Si consideri, ad esempio, lo scenario in cui un sistema di riconoscimento facciale operante *in tempo reale* in un ambiente liberamente accessibile al pubblico rilevi e processi una serie di volti, senza tuttavia individuare corrispondenze utili rispetto agli obiettivi predefiniti. In simili circostanze, risulterebbe in linea con il principio di *limitazione della conservazione* l'impiego di una tecnologia capace di eliminare

---

[112] Cfr. l'art. 5, par. 1, lett. *e*), GDPR, e dall'art. 4, par. 1, lett. e), LED.

[113] Cfr. C. eur., *S. & Marper*, cit., § 125.

[114] CGUE 30 gennaio 2024, C-118/22, § 69.

in maniera automatica dai propri archivi i dati raccolti ma non associati a risultati significativi [115]. Tale approccio, da un lato, consentirebbe di ridurre al minimo la registrazione non necessaria di informazioni personali, mitigando i rischi legati a un trattamento eccedente rispetto alla finalità perseguita; dall'altro, garantirebbe l'archiviazione esclusiva delle corrispondenze effettive, corredate da percentuali di similarità, assicurando una gestione dei dati mirata e specifica. Ovviamente, nel caso di corrispondenza, la conservazione del dato dovrebbe avvenire per il tempo strettamente necessario agli scopi definiti per i quali sussiste un fondamento legittimo [116]. Questo modello operativo rifletterebbe il principio di limitazione della conservazione dei dati e rafforzerebbe la fiducia nell'adozione di tecnologie avanzate, dimostrando come l'innovazione possa essere conforme al rispetto dei diritti fondamentali [117]. Tale problematica emerge con particolare vigore con riferimento all'archiviazione dei *templates* biometrici, ovvero le rappresentazioni digitali dei tratti biometrici di un individuo utilizzate per il confronto e l'identificazione nei sistemi di riconoscimento facciale e di autenticazione biometrica. Sul punto, la dottrina scientifica non ha assunto una posizione univoca, dando luogo a un acceso dibattito circa il livello di anonimizzazione garantito da tali modelli elettronici. Da una parte, alcuni studiosi sostengono che i *templates* biometrici, essendo ottenuti attraverso un processo di estrazione e codifica delle caratteristiche salienti del volto o di altre impronte biometriche, non consentano in alcun modo di risalire direttamente all'identità del soggetto di riferimento, poiché il dato originale viene trasformato in una rappresentazione cifrata priva di correlazione immediata con l'individuo [118]. Dall'altra, numerosi studi empirici hanno dimostrato come, nella pratica, il procedimento di digitalizzazione e archiviazione dei dati biometrici risulti quantomeno parzialmente reversibile, permettendo, attraverso specifiche tecniche di *reverse engineering*, di ricostruire in modo più o meno preciso l'immagine originaria del soggetto [119]. Ciò significa che, contrariamente a quanto

---

[115] Cfr. *infra* il § 4.3. S. QUATTROCOLO, *Intelligenza artificiale e processo penale: le novità dell'AI ACT*, in *Dir. dif.*, 16 gennaio 2025, p. 10.

[116] *Guidelines on Facial Recognition*, T-PD(2020)03rev4, 28 gennaio 2021, p. 12.

[117] Si tornerà su questo più avanti, cfr. capp. V, § 5 e VI, § 3.

[118] Cfr. C. PRINS, *Biometric Technology Law, Making Our Body Identify for us: Legal Implications of Biometric Technologies*, in *Computer Law and Security Report* 159, 14(3), 1998, p. 163; J. GRIJPINK, *Privacy Law: Biometrics and Privacy*, in *Computer Law & Security Review 154*, 17(3), 2001, p. 156-157 ss.

[119] Cfr. M. BROMBA, *On the Reconstruction of Biometric Raw Data from Template Data*,

sostenuto da alcune teorie, i *templates* biometrici non garantiscono un anonimato assoluto, ma conservano un legame con il dato originario che, in determinate circostanze e con l'impiego di strumenti adeguati, può essere riattivato.

Connesso alla limitazione e alle modalità di conservazione dei dati, il *principio di sicurezza* stabilisce che il trattamento debba avvenire in modo da garantire la massima tutela contro la perdita, la distruzione o il danneggiamento accidentale dei dati [120]. Il responsabile del trattamento è tenuto ad adottare diverse misure durante la trasmissione e la conservazione delle informazioni, come, per esempio, conservare i modelli biometrici e i dati grezzi in banche dati distinte, definire una politica di cifratura dei modelli elettronici biometrici o vietare qualsiasi accesso esterno [121]. Con riferimento a tali aspetti, l'introduzione di sistemi di sicurezza particolarmente rigidi nella gestione delle informazioni biometriche solleva interrogativi sotto il profilo del diritto di difesa, in particolare in relazione alla possibilità per l'indagato di accedere agli strumenti di riconoscimento facciale utilizzati a suo carico nel procedimento penale.

La rigorosa protezione dei dati biometrici, pur essendo essenziale per prevenire abusi e garantire la sicurezza delle informazioni, non dovrebbe tradursi in un ostacolo per l'esercizio del diritto di difesa. Affinché quest'ultimo non risulti compromesso, sarebbe necessario prevedere meccanismi di *audit* e di verifica indipendente, che consentano agli esperti (nominati d'ufficio o dalle parti) di analizzare l'affidabilità e la correttezza degli algoritmi impiegati nel riconoscimento facciale. Tale esigenza è particolarmente rilevante alla luce dei ben noti problemi di *bias*, che possono influenzare l'esito del riconoscimento e condurre a errori di identificazione [122].

A chiusura della rassegna delle disposizioni previste dalla direttiva, merita di soffermarsi sul *principio di accountability*, il quale prescrive che il responsabile del trattamento dei dati sia tenuto a dimostrare il rispetto dei principi di protezione [123], con l'obiettivo di anticipare la tutela ad un

---

2006, https://www.bromba.com/knowhow/temppriv.htm e A. ROSS-J. SHAH-A. JAIN, *From Template to Image: Reconstructing Fingerprints from Minutiae Points*, in *IEEE Transactions on Patterns Analysis and Machine Intelligence*, 29(4), 2007, p. 544.

[120] Cfr. l'art. 4, par. 1, lett. f), LED.

[121] Cfr. EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Regulating facial recognition in the EU*, cit., p. 17.

[122] Cfr. il capitolo II, § 4.6.

[123] Cfr. l'art. 4, par. 4 LED e art. 5, par. 2 GDPR.

momento precedente al trattamento e a prevenire così eventuali possibili violazioni [124]. In base a questo principio, il responsabile del trattamento non solo deve conformarsi alla normativa posta a protezione dei dati, tramite procedure e misure tecnico-organizzative, ma anche dimostrare tale conformità. L'applicazione del principio di *accountability* nell'impiego di strumenti di riconoscimento facciale impone che ogni fase del procedimento – dall'acquisizione delle immagini al trattamento tramite software, dall'estrazione delle caratteristiche biometriche fino alla successiva archiviazione del *template* – sia soggetta a un controllo strutturato e documentato, in grado di garantire che il trattamento avvenga nel rispetto dei principi di necessità, proporzionalità e minimizzazione.

In questo senso, diventa imprescindibile la predisposizione di una valutazione d'impatto sulla protezione dei dati (DPIA), volta a identificare e a mitigare i rischi associati all'uso della tecnologia biometrica, garantendo che eventuali criticità siano individuate e affrontate prima dell'effettiva implementazione del sistema [125]. Accanto alla valutazione d'impatto, la direttiva prevede la necessità di una consultazione preventiva con l'Autorità garante per la protezione dei dati personali, la quale ha il compito di esprimere un parere sulla liceità del trattamento, soprattutto nei casi in cui l'utilizzo del riconoscimento facciale possa presentare rischi elevati per i diritti e le libertà fondamentali degli interessati.

Un ulteriore obbligo in capo al responsabile del trattamento riguarda il monitoraggio e la documentazione delle attività di gestione delle informazioni trattate [126], con particolare riguardo alla registrazione delle operazioni di accesso, modifica e conservazione dei dati biometrici. La tracciabilità delle operazioni consente non solo di garantire la trasparenza delle attività di trattamento, ma anche di fornire un riscontro oggettivo in caso di verifiche da parte delle autorità competenti.

---

[124] A. MANTELERO, *La gestione del rischio*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, Zanichelli, Bologna, 2019, p. 473 ss.; G. SARTOR-F. LAGIOIA, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, European Parliament, Bruxelles, 2020, p. 66.

[125] Cfr. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, cit., p. 26; INFORMATION COMMISSIONER'S OFFICE, *Opinion on the use of live facial recognition technology by law enforcement in public places*, 2019, p. 13-14; EUROPEAN DATA PROTECTION BOARD, *Guidelines 3/2019 on processing of personal data through video devices*, 2020, p. 33.

[126] Cfr. l'art. 24 LED.

4.3. *Approcci giurisprudenziali stranieri all'impatto del riconoscimento facciale sul diritto alla riservatezza: il procedimento inglese* Ed Bridges (R) *c.* The Chief Constable of South Wales Police

Come anticipato, il recente emergere delle problematiche all'attenzione impone di volgere lo sguardo non solo alle indicazioni provenienti dalle Corti europee, ma anche agli orientamenti giurisprudenziali formatisi in altri ordinamenti. Sebbene in nessun Paese europeo paia ancora esistere un paradigmatico *case law* [127], sembra utile richiamare la giurisprudenza d'Oltremanica che, per la prima volta, ha approfondito l'analisi degli strumenti di riconoscimento facciale nello spettro di alcuni principi poc'anzi richiamati.

Dapprima la *High Court of Justice of England and Wales* [128] e, successivamente in sede di impugnazione, la *Court of Appeal* [129] si sono pronunciate sulla possibilità di impiego del cd. "*Automated Facial Recognition Locate*"

---

[127] Cfr. FUNDAMENTAL RIGHTS AGENCY, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., p. 4. Cfr. anche M. ZALNIERIUTE, *Burning Bridges: the automated facial recognition technology and public space surveillance in the modern State*, in *Colum. Sci. & Tech. L. Rev.*, 22, 2021, p. 288.

[128] Cfr. HIGH COURT OF JUSTICE, *Queen's Bench Division, Divisional Court*, 4 settembre 2019, Case No: CO/4085/2018, R (Bridges) v. CCSWP e SSHD (d'ora in avanti: [2019] EWHC 2341 (Admin)). Cfr. J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del Garante privacy d'Oltremanica)*, in *Sist. pen.,* 28 marzo 2020; A. PIN, *Non esiste la "pallottola d'argento": l'Artificial Face Recognition al vaglio giudiziario per la prima volta*, in *DPCE Online*, 41(4), 2020; I. BORSHOFF, *UK Court backs police in facial recognition lawsuit*, 2019, https://www.politico.eu/article/uk-court-backs-police-in-facial-recognition-lawsuit/; E. FALETTI, *Face detection: per la prima volta il riconoscimento al vaglio dei tribunali*, in *Quot. giur.*, 29 ottobre 2019.

[129] Cfr. COURT OF APPEAL, R (Bridges) v. CCSWP e SSHD (d'ora in avanti: [2020] EWCA Civ 1058). Cfr. M. ZALNIERIUTE, *Burning Bridges: the automated facial recognition technology and public space surveillance in the modern State*, cit., p. 284 ss.; G.K.Y. CHAN, *Towards a calibrated trust-based approach to the use of facial recognition technology*, in *International Journal of Law and Information Technology*, 2021, p. 13 ss. e B. KEENAN, *Automatic Facial Recognition and the Intensification of Police Surveillance*, in *Modern Law Review*, 2021, 84(4), p. 886-897. Cfr. anche "*Surveillance Camera Commissioner's statement: Court of Appeal judgment (R) Bridges v South Wales Police – Automated Facial Recognition*", reperibile su https://www.gov.uk/government/speeches/surveillance-camera-commissioners-statement-court-of-appeal-judgment-r-bridges-v-south-wales-police-automated-facial-recognition, "*UK Court of Appeal Finds Automated Facial Recognition Technology Unlawful in Bridges v South Wales Police*", reperibile su https://www.huntonprivacyblog.com/2020/08/12/uk-court-of-appeal-finds-automated-facial-recognition-technology-unlawful-in-bridges-v-south-wales-police/.

(*AFRL*) [130], uno strumento di riconoscimento facciale *in tempo reale*, in dotazione alla *South Wales Police*, nell'ambito della realizzazione di un progetto pilota per finalità di sicurezza [131]. Quest'ultimo, tra diversi programmi intrapresi nel Regno Unito, è stato avviato in assenza di una disciplina legislativa di riferimento che regolamentasse specificamente tale attività di tracciamento [132].

Il ricorrente, nel caso di specie, lamentava di essere stato sottoposto, in modo illegittimo, all'impiego di un software di riconoscimento facciale *in tempo reale*, mentre si trovava nella città di Cardiff [133]. La *South Wales Police*, secondo le doglianze dell'interessato, avrebbe impiegato tale strumento in assenza di una disciplina normativa autorizzativa *ad hoc:* da ciò sarebbero dunque derivate la lesione del suo diritto alla riservatezza, la violazione della disciplina eurounitaria e interna in materia di protezione dei dati personali, nonché l'inosservanza di alcune disposizioni dell'*Equality Act* [134], potendo la tecnologia in esame, secondo il ricorrente, concretizzare il rischio di generare *bias* cognitivi [135] discriminatori nei confronti di donne e minoranze etniche [136].

Peraltro, non era noto né al ricorrente, né alla polizia, né alla Corte se costui fosse stato effettivamente ripreso dalla telecamera [137]. Infatti, in mancanza di *match*, il software era stato programmato per eliminare automaticamente i dati biometrici raccolti [138].

---

[130] Da ora in avanti "*AFRL*".

[131] *Algorithm use in the criminal justice system*, https://www.lawsociety.org.uk/topics/research/algorithm-use-in-the-criminal-justice-system-report.

[132] Cfr. B. KEENAN, *Automatic Facial Recognition and the Intensification of Police Surveillance*, in *Modern Law Review*, 84(4), 27 febbraio 2021 e J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, cit., p. 7.

[133] Cfr. [2019] EWHC 2341 (Admin), § 11 ss.

[134] Si tratta della legislazione antidiscriminatoria britannica volta a tutelare il diritto di tutti gli individui a godere di pari opportunità in ogni ambito della vita. Cfr. https://www.gov.uk/guidance/equality-act-2010-guidance.

[135] Cfr. A. TURING, *Intelligenza meccanica*, Bollati Boringhieri, Torino, 1994.

[136] Cfr. [2019] EWHC 2341 (Admin), § 20. Per un approfondimento v. FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27 novembre 2019, p. 4 e EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Regulating facial recognition in the EU*, September 2021, p. 13 ss.

[137] Cfr. [2019] EWHC 2341 (Admin), § 16. Cfr. J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del Garante Privacy D'Oltremanica)*, in *Sist. pen.*, 28 marzo 2020, p. 3.

[138] Cfr. [2019] EWHC 2341 (Admin), § 16.

La *High Court of Justice* ha innanzitutto riconosciuto che l'utilizzo del software di riconoscimento facciale da parte della polizia gallese ha comportato un'ingerenza nella vita privata del ricorrente, potenzialmente lesiva dell'art. 8 della Conv. eur. dir. uomo, in quanto il rilievo e l'estrazione del profilo facciale costituiscono «*information of an "intrinsically private" character*» [139]. Tuttavia, tale ingerenza nella sfera privata è stata ritenuta legittima, poiché il paragrafo 2 della citata disposizione prevede che le autorità pubbliche possano compiere un'intrusione nella vita privata dei singoli, laddove tale attività sia prevista «dalla legge e costituisca una misura che, in una società democratica, [sia] necessaria alla sicurezza nazionale, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

I giudici britannici hanno affermato che l'attività di raccolta e conservazione dei dati biometrici facciali mediante algoritmi di riconoscimento rientra nell'alveo dei poteri generali attribuiti alle forze di polizia, finalizzati alla prevenzione e al contrasto della criminalità. In particolare, il ricorso legittimo agli strumenti di *facial recognition* troverebbe il suo fondamento non solo nelle disposizioni generali in materia di protezione dei dati personali [140], ma anche in una serie di norme di rango regolamentare, concernenti la videosorveglianza e le *local policies* adottate dalla *South Wales Police* [141].

Oltre a ciò, le tecnologie di riconoscimento facciale non sarebbero così intrusive come, per esempio, il prelievo di campioni biologici finalizzati all'estrazione del DNA o il rilievo delle impronte digitali, dal momento che «*no physical entry, contact or force is necessary when using AFR Locate to obtain biometric data*» [142].

---

[139] Cfr. [2019] EWHC 2341 (Admin), § 57. Lo stesso approccio – prosegue la *High Court* – si riscontra anche nel *case-law* della Corte di Giustizia dell'Unione europea, la quale, nel caso *Schwarz*, ha posto in relazione l'acquisizione di *fingerprints and facial images* con il diritto al «rispetto della vita privata con riguardo al trattamento dei dati personali», che concerne «ogni informazione relativa ad una persona fisica identificata o identificabile». CGUE, 17 ottobre 2013, *Schwarz*, C-291/12, § 48.

[140] Cfr. [2019] EWHC 2341 (Admin), § 84 ss. In particolare, il *Data Protection Act* del 2018 «(…) *embeds key safeguards which apply to all processing of all personal data – including the biometric data processed when AFR Locate is used*», § 85.

[141] La Corte si riferisce al "*Surveillance Camera Code of Practice*" e ad altri tre provvedimenti di rango non legislativo, il *SWP's Standard Operating Procedure*, il *SWP's Deployment Reports* e il *SWP's Policy on Sensitive Processing* (v. i §§ 89 e 92).

[142] Cfr. [2019] EWHC 2341 (Admin), § 75.

Pertanto, secondo la Corte, non essendoci alcuna ingerenza fisica diretta sugli individui, allo stesso modo di quanto accade per le videoriprese [143], non sarebbe necessario che le autorità di *law enforcement* siano dotate di «*new express statutory powers*» per potersi avvalere dei software di riconoscimento facciale *in tempo reale* [144].

Con riferimento alla seconda doglianza del ricorrente, concernente la violazione della disciplina generale della tutela della riservatezza, la Corte ha osservato che il procedimento di riconoscimento era stato condotto al fine di perseguire lo scopo di prevenzione e contrasto della criminalità, in modo del tutto conforme alla normativa (interna ed eurounitaria) in materia di trattamento dei dati personali [145].

In particolare, le autorità di polizia avrebbero predisposto garanzie particolarmente elevate rispetto alla *data retention* [146], informando la popolazione «*about AFRL and as to its use at the event or in the area which they may be attending or present*» [147]. Oltre a ciò, prima di procedere con l'attività di *facial recognition* mediante videoripresa, la polizia gallese avrebbe adottato il programma denominato "*Policy on Sensitive Processing for Law Enforcement Purposes*" [148], avente ad oggetto le attività compiute per «*securing compliance with the data protection principles*» [149] e un "*Data Protection Impact Assessment*" [150], tramite il quale veniva chiarito l'esatto funzionamento del sistema "*AFR Locate*" e i rischi per la protezione dei dati personali.

Infine, quanto ai potenziali effetti discriminatori della tecnologia nei confronti di minoranze etniche e di genere, la Corte ha ritenuto che, nel caso di specie, non vi fosse «*firm evidence that the software does produce results that*

---

[143] Cfr. [2019] EWHC 2341 (Admin), §§ 73 e 75, ove la Corte, riferendosi ai software di riconoscimento facciale, specifica che «*the method is no more intrusive than the use of CCTV in the streets*».

[144] Cfr. [2019] EWHC 2341 (Admin), § 78.

[145] Cfr. [2019] EWHC 2341 (Admin), §§ 122 ss., 133 ss., 139 ss. e 144 ss.

[146] Cfr. [2019] EWHC 2341 (Admin), § 37 ss. ove la Corte specifica che «(…) *if no match (false or positive) is made – as in the overwhelming majority of cases – then AFR Locate does not retain the facial biometrics or image of persons whose faces are scanned. They are immediately and automatically deleted. That data is not available to the system operator or any other police officer*».

[147] Cfr. [2019] EWHC 2341 (Admin), § 39.

[148] Cfr. [2019] EWHC 2341 (Admin), § 139.

[149] Cfr. [2019] EWHC 2341 (Admin), § 138.

[150] Cfr. [2019] EWHC 2341 (Admin), § 147 ss.

suggest indirect discrimination»[151]. La *South Wales Police* aveva peraltro adottato un ulteriore provvedimento, l'"*Equality Impact Assessment – Initial Assessment*"[152], con il quale erano stati calcolati i rischi di eventuali discriminazioni derivanti dall'uso del software *de quo.* Questo documento, unitamente ad una dichiarazione di un funzionario della Divisione Servizi digitali[153] nella quale venivano fornite informazioni sul tasso di false corrispondenze, ha condotto i giudici a ritenere che la *South Wales Police* avesse agito legittimamente.

La decisione in esame ha suscitato diverse critiche da parte dell'*Information Commissioner's Office*, Autorità garante per la protezione dei dati personali locale[154]. In primo luogo, in diversi documenti[155], l'*ICO* ha sottolineato i rischi attualmente esistenti legati all'impiego in luoghi aperti al pubblico della tecnologia di *live facial recognition* da parte delle forze di polizia nel Regno Unito. In particolare, l'Autorità ha affermato che tale software dovrebbe essere impiegato solamente in presenza di «*specific serious or violent crimes*»[156] e non anche per forme di reato bagatellari. Oltre a ciò, dovrebbe essere sempre necessario specificare le ragioni per le quali non è possibile ricorrere a mezzi investigativi alternativi e meno invasivi[157]. In questa prospettiva, l'*ICO* ha colto l'occasione per invitare le autorità governative ad adottare «*a statutory binding code of practice to provide further safeguards that address the*

---

[151] Cfr. [2019] EWHC 2341 (Admin), § 153.

[152] Cfr. [2019] EWHC 2341 (Admin), § 158.

[153] Cfr. [2019] EWHC 2341 (Admin), § 154.

[154] Da qui in avanti "*ICO*".

[155] Cfr. INFORMATION COMMISSIONER'S OPINION, "*Live facial recognition technology – police forces need to slow down and justify its use*", reperibile su https://ico.org.uk/about-the-ico/news-and-events/blog-live-facial-recognition-technology-police-forces-need-to-slow-down-and-justify-its-use/; "*ICO investigation into how the police use facial recognition technology in public places*", reperibile su https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf; INFORMATION COMMISSIONER'S OPINION, "*The use of live facial recognition technology by law enforcement in public places*", reperibile su https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

[156] Cfr. INFORMATION COMMISSIONER'S OPINION, "*The use of live facial recognition technology by law enforcement in public places*", cit., p. 15. Negli stessi termini, cfr. anche EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), *Facial recognition technology*, cit., p. 34.

[157] Cfr. INFORMATION COMMISSIONER'S OPINION, "*The use of live facial recognition technology by law enforcement in public places*", cit., p. 15.

specific issues arising from the use of biometric technology such as LFR» [158].

La pronuncia della *Queen's Bench Division* della *High Court of Justice* è stata successivamente impugnata dinanzi alla *Civil Division della Court of Appeal*, che, con sentenza dell'11 agosto 2020, ha riformato la decisione di primo grado. Entrambe le Corti hanno ritenuto che l'impiego del sistema *AFR Locate* interferisca con il diritto al rispetto della vita privata. A differenza di quanto affermato dai giudici di primo grado che hanno ritenuto l'impiego del sistema *AFR Locate* riconducibile ai «*common law powers*» della polizia, la *Court of Appeal* ha sviluppato le proprie argomentazioni sulla base di presupposti giuridici differenti, giungendo a conclusioni di segno opposto [159]. Secondo i giudici di seconde cure, infatti, l'«*AFR as a novel technology* (…) *involves the capturing of the images and processing of digital information of a large number of members of the public, in circumstances in which it is accepted that the vast majority of them will be of no interest whatsoever to the police*». La normativa attualmente esistente non sarebbe sufficientemente specifica per rispondere all'interrogativo su chi effettivamente possa essere inserito nelle *watchlist* e in quali luoghi tali sistemi possano essere collocati e attivati. A tal proposito, di particolare rilevanza sono state le considerazioni della Corte d'Appello in merito alla necessità dell'intervento di un magistrato nell'autorizzare l'uso dell'*AFR Locate* [160].

L'argomentazione della *Court of Appeal* si fonda sulla considerazione che l'inserimento nelle *watchlists* comporta una forma di trattamento dei dati altamente invasiva, che incide non solo sulla tutela della riservatezza del singolo individuo, ma anche sulla libertà di movimento e sull'autodeterminazione personale. L'assenza di una previa autorizzazione da parte di un organo giurisdizionale rischia di tradursi in una sorveglianza selettiva su base arbitraria, in cui la scelta dei soggetti da sottoporre a identificazione biometrica rimane affidata esclusivamente alla discrezionalità delle autorità di polizia.

Con riferimento alla necessità di minimizzare il rischio di effetti discriminatori derivanti dall'impiego delle tecnologie di riconoscimento facciale, la *Court of Appeal* ha sottolineato che le autorità pubbliche sono tenute a compiere tutte le verifiche necessarie per valutare l'impatto potenziale di tali

---

[158] Cfr. INFORMATION COMMISSIONER'S OPINION, "*The use of live facial recognition technology by law enforcement in public places*", cit., p. 21.

[159] Cfr. [2020] EWCA Civ. 1058 § 86 ss.

[160] Cfr. [2020] EWCA Civ. 1058, § 126.

strumenti, soprattutto quando il loro utilizzo potrebbe generare effetti negativi nei confronti di specifiche categorie di individui. Questo principio si inserisce nell'alveo del più generale obbligo di *due diligence* che grava sulle pubbliche amministrazioni nell'adozione di sistemi tecnologici potenzialmente lesivi dei diritti fondamentali, imponendo un'attenta analisi delle conseguenze discriminatorie che potrebbero derivare dal funzionamento dell'algoritmo.

In questa prospettiva, secondo i giudici d'appello, per valutare in modo adeguato la proporzionalità dell'impiego dell'*AFR Locate*, sarebbe necessario disporre di dati affidabili circa la distribuzione dei falsi positivi e dei falsi negativi all'interno di gruppi distinti, ad esempio tra donne e uomini. Tuttavia, tale operazione risulta estremamente complessa, in quanto il sistema era stato progettato per eliminare automaticamente i dati considerati incompatibili, rendendo impossibile un'analisi retrospettiva delle performance dell'algoritmo rispetto a variabili demografiche specifiche [161].

La *Court of Appeal* ha infine stabilito che «*the Respondent's use of Live Automated Facial Recognition technology was not in accordance with the law for the purposes of Article 8(2), (…) did not comply with section 64(3)(b) and (c) of the Data Protection Act 2018 (…)*» e «*did not comply with the Public Sector Equality Duty in section 149 of the Equality Act 2010 (…)*» [162].

I giudici, anziché sottolineare la necessità di un'armonizzazione normativa su scala nazionale, hanno ritenuto sufficiente demandare a ciascun dipartimento di polizia la predisposizione di linee guida autonome per la regolamentazione dell'uso delle tecnologie di riconoscimento facciale. Una simile impostazione rischia di generare una frammentazione normativa, creando disparità applicative tra diverse aree geografiche e aumentando l'incertezza in merito ai limiti e alle garanzie che dovrebbero disciplinare l'impiego di tali strumenti. Sarebbe stato più opportuno promuovere l'elaborazione di un quadro normativo unitario e vincolante, capace di limitare la discrezionalità delle autorità di polizia e di prevenire potenziali violazioni dei diritti fondamentali.

In questa prospettiva, per mitigare il rischio di abusi, il *Surveillance Camera Commissioner* [163] ha formulato una serie di principi guida per un

[161] Cfr. [2020] EWCA Civ. 1058, § 191.

[162] Cfr. [2020] EWCA Civ. 1058, § 210.

[163] Il *Surveillance Camera Commissioner*, ente del Regno Unito che vigila sull'utilizzo dei sistemi di videosorveglianza.

impiego responsabile e proporzionato della tecnologia da parte delle forze dell'ordine [164].

In primo luogo, il ricorso ai sistemi di riconoscimento facciale deve essere subordinato a una giustificazione chiara e rigorosa, garantendo che ogni applicazione sia proporzionata agli obiettivi perseguiti e sottoposta a un processo di valutazione trasparente. È essenziale, inoltre, che le decisioni basate su tali tecnologie prevedano sempre un intervento umano, evitando forme di determinazione automatizzata.

Un altro aspetto cruciale concerne l'affidabilità dei dati biometrici utilizzati, spesso derivanti da database di terze parti. Il *Surveillance Camera Commissioner* ha enfatizzato l'importanza di verificare periodicamente la qualità dei dati impiegati per ridurre il rischio di errori, discriminazioni e falsi positivi, che potrebbero compromettere la legittimità delle operazioni di sorveglianza.

Nel caso dell'impiego del riconoscimento facciale *in tempo reale*, i responsabili delle forze di polizia devono chiarire e rendere pubblici i criteri di selezione delle persone incluse nelle liste di controllo, garantendo trasparenza e *accountability* nell'applicazione della tecnologia. Inoltre, i dati biometrici raccolti che non generano *alert* correlati a soggetti nelle *watchlist* devono essere cancellati immediatamente, in conformità con il principio di minimizzazione dei dati, limitando il trattamento esclusivamente alle informazioni necessarie e proporzionate rispetto alle finalità perseguite.

L'obbligo di cancellazione immediata nel caso di un mancato *match* fra i dati introduce un elemento di garanzia fondamentale nella gestione dei dati biometrici, ridefinendo i termini del bilanciamento tra sicurezza e tutela della riservatezza. Il divieto di conservazione indiscriminata dei dati non solo limita il rischio di profilazione massiva e sorveglianza generalizzata, ma previene anche possibili utilizzi impropri o non autorizzati delle informazioni biometriche raccolte. Questa impostazione mira a contenere la pervasività della tecnologia di riconoscimento facciale, evitando la formazione di archivi biometrici sovradimensionati che potrebbero esporre gli individui a un controllo costante e in contrasto con il principio di proporzionalità. Da un punto di vista tecnologico e normativo, tale prescrizione incide in maniera

---

[164] "*Facing the Camera Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, Public Places in England & Wales*", https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf.

significativa sulla prospettiva di utilizzo del riconoscimento facciale, enfatizzandone l'uso selettivo e mirato. L'eliminazione tempestiva dei dati non rilevanti favorisce, infatti, una maggiore accettabilità sociale della tecnologia, contribuendo a consolidarne l'inquadramento entro schemi regolatori ben definiti.

Particolare attenzione poi deve essere posta alla possibile discriminazione algoritmica, con specifico riferimento ai gruppi minoritari o vulnerabili, per evitare che l'intelligenza artificiale riproduca *bias* sistemici, amplificando disparità e ingiustizie sociali. Gli algoritmi e i database impiegati devono essere testati e monitorati regolarmente, attraverso procedure di *auditing* indipendenti, per garantire accuratezza, equità e imparzialità nelle identificazioni biometriche.

Infine, l'utilizzo del riconoscimento facciale deve essere subordinato a un processo di autorizzazione formale, con criteri chiari per la concessione delle autorizzazioni e la definizione delle circostanze specifiche in cui tali tecnologie possono essere impiegate. A questo proposito, un aspetto cruciale di tale disciplina è rappresentato dalla tracciabilità della catena di responsabilità istituzionale. L'impiego delle tecnologie di riconoscimento facciale deve essere documentato, monitorato e sottoposto a un sistema di verifica indipendente, al fine di garantire che il loro utilizzo sia conforme alle finalità per cui è stato autorizzato e non sfoci in forme di sorveglianza massiva o utilizzi impropri. La creazione di meccanismi di controllo strutturati e trasparenti, che prevedano *audit* periodici e sistemi di *reporting*, è indispensabile per evitare abusi e garantire una piena *accountability* delle autorità preposte. In questo contesto, la previsione di procedure autorizzative rigorose e l'istituzione di meccanismi di supervisione indipendenti costituiscono strumenti fondamentali per bilanciare l'innovazione tecnologica con la tutela delle libertà individuali, assicurando che il riconoscimento facciale venga utilizzato esclusivamente in contesti giuridicamente giustificati e con adeguate garanzie di protezione dei dati personali.

4.4. *(Segue) L'affaire* Glukhin c. Russia*: prime indicazioni da Strasburgo*

Più di recente, con la decisione *Glukhin c. Russia*[165], la Corte di Strasburgo per la prima volta affronta, in maniera articolata, il tema dell'impiego

[165] C. eur. 4 luglio 2023, *Glukhin c. Russia*, 11519/20. Per un approfondimento cfr. F. PALMIOTTO-N. MENÉNDEZ GONZÁLEZ, *Facial recognition technology, democracy and human*

del riconoscimento facciale tramite software, come strumento per la raccolta di informazioni nell'ambito di un procedimento amministrativo [166]. La pronuncia – che si inserisce in un quadro giurisprudenziale ancora in fase di definizione – presenta rilevanti implicazioni sistemiche, non solo in relazione al rapporto tra sorveglianza algoritmica e libertà fondamentali, ma anche rispetto alla tenuta del principio di legalità quale parametro imprescindibile per la legittimità dell'azione amministrativa.

Nel caso di specie, il ricorrente era stato identificato e sottoposto a detenzione amministrativa per aver omesso la comunicazione preventiva alle autorità dell'intenzione di svolgere una dimostrazione individuale, come previsto dall'art. 20, comma 2, par. 5 del Codice degli illeciti amministrativi della Federazione Russa. Attraverso l'impiego delle tecnologie di riconoscimento facciale installate nelle stazioni della metropolitana [167] e, mediante la visualizzazione di taluni audio e video diffusi sui canali pubblici di *Telegram*, l'unità anti-estremismo della polizia di Mosca era riuscita a riconoscere proprio il ricorrente, al quale veniva contestata la violazione della vigente procedura amministrativa. In particolare, la polizia aveva ritenuto che l'oggetto utilizzato dall'attivista nel corso della manifestazione – una sagoma di cartone – rientrasse nella categoria dei «*quickly (de)assembled objects*» [168], per l'uso dei quali la normativa vigente impone l'obbligo di preavviso anche nel contesto di dimostrazioni individuali. In conseguenza, Glukhin veniva ritenuto responsabile dell'illecito e condannato al pagamento di una sanzione pecuniaria di 20.000 rubli.

L'interessato impugnava il provvedimento amministrativo, deducendo la

---

rights, in *50 Computer Law & Security Review,* 3, 2023; M. ZALNIERIUTE, *Glukhin v. Russia. App. No. 11519/20. Judgment*, in *American Journal of International Law*, 117(4), 2023, p. 699; I. NERONI REZENDE, *Glukhin and the EU regulation of facial recognition: Lessons to be learned?*, in *European Law Blog*, 19 settembre 2023; G. MOBILIO, *La Corte EDU condanna il ricorso alle tecnologie di riconoscimento facciale per reprimere il dissenso politico: osservazioni a partire dal caso Glukhin c. Russia*, in *DPCE Online*, 62(1), 2024.

[166] C. eur., *Glukhin c. Russia*, cit., § 83.

[167] Come sottolineano F. PALMIOTTO-N. MENENDEZ, *Facial recognition technology, democracy and human rights*, in *CL&SR*, 50, 2023: «*the applicant could only presume that FRT was used in his case, as domestic law did not require the police to record their use of FRT or notify individuals affected by it. At the same time, however, he was identified within "less than two days" after his demonstration and precisely located at the underground station after only one hour since the police did not find him in his house.* (…) *In the police reports, however, there is no trace or mention of the use of FRT*».

[168] L. n. FZ-54 del 19 giugno 2004, sezione 7(1.1).

violazione della libertà di espressione, ribadendo di aver preso parte a una manifestazione pacifica e sostenendo di aver subito una sanzione ingiusta. Nello specifico, il ricorrente eccepiva l'illegittimità delle attività di identificazione condotte dalla polizia, argomentando che la normativa interna non contemplasse la possibilità di svolgere tali operazioni a fini identificativi. La censura sollevata mirava dunque a evidenziare il contrasto tra l'azione delle autorità di polizia e il principio di legalità, ponendo l'accento sulla mancanza di un quadro normativo chiaro e rispettoso delle garanzie fondamentali.

I giudici d'appello respingevano il ricorso, confermando la decisione nei confronti di Glukhin, poiché la raccolta degli elementi identificativi [169] sarebbe avvenuta in conformità con quanto contemplato dalla legge amministrativa russa [170].

Esauriti senza successo i gradi di giudizio previsti dall'ordinamento interno, l'interessato adiva la Corte europea dei diritti dell'uomo nel gennaio 2020, deducendo la violazione degli articoli 8 e 10 della Convenzione. Il ricorrente contestava l'ingerenza delle autorità nella propria sfera privata, in quanto l'identificazione era avvenuta mediante tecniche di riconoscimento facciale, senza un'adeguata base giuridica e in assenza delle garanzie procedurali sufficienti a prevenire un uso arbitrario dello strumento. Parallelamente, egli lamentava la compressione del diritto alla libertà di espressione, sostenendo che la sanzione irrogata – solo in virtù dell'impiego di strumenti di riconoscimento facciale – per la sua partecipazione alla manifestazione pacifica avesse avuto un effetto dissuasivo sull'esercizio del diritto di riunione e sulla libera manifestazione del pensiero. L'azione delle autorità, secondo il ricorrente, non sarebbe risultata conforme ai requisiti di necessità e proporzionalità previsti dall'art. 10, poiché l'intervento repressivo non rispondeva a un interesse pubblico prevalente, né si giustificava in relazione alla tutela dell'ordine pubblico.

Una volta chiarita la sussistenza della giurisdizione della Corte di Strasburgo per la questione in esame [171], la medesima ha innanzitutto ricordato

---

[169] A tal proposito, il capitolo 26 del Codice sugli illeciti amministrativi dispone che documenti, registrazioni, audio e video e qualsiasi altro dato sensibile possono sempre essere impiegati come prove nei procedimenti amministrativi se contengono informazioni rilevanti ai fini della decisione.

[170] La legge in discorso (l. n. 3-FZ del 7 febbraio 2011) prevede, in generale, che la polizia adotti misure atte a individuare e perseguire gli illeciti amministrativi di sua competenza nonché misure miranti a prevenire e reprimere le attività estremiste.

[171] Le presunte violazioni si sarebbero verificate antecedentemente al 16 settembre 2022,

che la tutela garantita dall'art. 10 non si esaurisce nella protezione della mera espressione verbale o scritta di un determinato pensiero. Al contrario, la norma convenzionale si estende a qualsiasi forma di manifestazione di idee, comprendendo anche modalità non verbali di comunicazione, quali simbolismi, gestualità o comportamenti idonei a veicolare un messaggio nell'ambito del dibattito pubblico. Del resto, la giurisprudenza della Corte ha costantemente riconosciuto che la libertà di espressione non si limita al contenuto del messaggio trasmesso, ma investe altresì le modalità attraverso cui esso viene comunicato [172]. Di conseguenza, la Corte ha proceduto ad un'analisi sulle condizioni alle quali sono ammesse limitazioni alla libertà di espressione [173]. In primo luogo, è necessario accertare che la misura limitativa sia «prevista dalla legge», ossia che l'interferenza sia fondata su una base normativa chiara, accessibile e prevedibile per i destinatari. La certezza del diritto impone che le restrizioni alla libertà di espressione non possano derivare da disposizioni generiche o indeterminate, ma debbano fondarsi su una previsione legislativa sufficientemente precisa, da consentire ai cittadini di conformare il proprio comportamento.

In secondo luogo, la limitazione deve perseguire almeno uno degli scopi indicati dalla norma convenzionale, tra cui la tutela della sicurezza nazionale, dell'ordine pubblico, della salute o della morale, nonché la protezione della reputazione o dei diritti altrui. La mera indicazione di un obiettivo astrattamente riconducibile a tali finalità non è sufficiente, dovendo l'ingerenza statale rispondere a una necessità concreta e attuale.

L'elemento decisivo dell'analisi si rinviene, infine, nel requisito della «necessità in una società democratica», secondo cui l'interferenza con la libertà di espressione deve essere giustificata dall'esistenza di un "bisogno sociale impellente" e risultare "proporzionata allo scopo perseguito". Ciò implica che la misura adottata dalle autorità non debba eccedere quanto strettamente necessario per conseguire il fine legittimo individuato, dovendo sussistere un equilibrio ragionevole tra l'interesse pubblico e la tutela dei diritti fondamentali dell'individuo.

---

data in cui la Federazione Russa ha cessato, come noto, di essere parte contraente della Convenzione europea dei diritti dell'uomo: i giudici hanno ritenuto il ricorso ammissibile poiché né manifestamente infondato né tanto meno irricevibile ai sensi dell'art. 35. Conv. eur. dir. uomo, Grande Camera, *Ucraina e Paesi Bassi c. Russia*, ric. 8019/16 (2022), § 435 ss.

[172] Cfr. C. eur. 26 aprile 2016, *Novikova e altri c. Russia*, nn. 25501/07 e altri 4, § 110 ss., *Silver e altri c. Regno Unito*, nn. 5947/72, 25 marzo 1983, § 87.

[173] C. eur., *Glukhin c. Russia*, cit., §§ 54-56.

In tale prospettiva, i giudici di Strasburgo hanno ritenuto che il ricorrente, alla luce delle circostanze del caso e del contesto fattuale in cui si sono svolti gli eventi, avesse esercitato legittimamente il proprio diritto a manifestare il pensiero, rientrando la sua condotta nell'ambito di protezione delineato dall'art. 10. La Corte ha osservato che la partecipazione dell'interessato alla manifestazione costituiva una forma di espressione politica, finalizzata a contribuire al dibattito su una questione di interesse pubblico, e come tale meritevole di tutela [174]. Il ricorrente aveva partecipato a una manifestazione individuale caratterizzata da modalità pacifiche e prive di qualsiasi profilo di pericolosità, senza che la sua condotta avesse in alcun modo compromesso l'ordine pubblico o integrato elementi di offensività.

L'unico addebito contestato concerneva la mancata comunicazione preventiva all'autorità competente, configurando quindi una violazione meramente formale, priva di implicazioni sostanziali in termini di sicurezza o ordine pubblico. Nonostante ciò, le autorità hanno adottato un approccio restrittivo che la Corte ha ritenuto carente del necessario grado di tolleranza richiesto in una società democratica, soprattutto in relazione alla tutela della libertà di espressione e di manifestazione del pensiero. Di conseguenza, sebbene l'ingerenza statale possa astrattamente ritenersi conforme alla normativa interna, in quanto finalizzata al perseguimento di obiettivi legittimi quali la tutela dell'ordine pubblico, la prevenzione dei reati o la salvaguardia della reputazione e dei diritti altrui, essa non soddisfa il requisito essenziale della "necessità" in una società democratica.

La Corte, però, ha concentrato maggiormente i suoi sforzi nell'analisi della presunta violazione del secondo parametro di riferimento, ossia l'art. 8. Più nel dettaglio, il ricorrente aveva evidenziato di essere stato ripreso dalle telecamere di videosorveglianza installate nella metropolitana di Mosca e successivamente identificato mediante l'impiego di un sistema di riconoscimento facciale, senza che vi fosse stata alcuna preventiva autorizzazione da parte delle competenti autorità statali [175]. Glukhin, infatti, aveva meramente dedotto che fosse stata utilizzata la tecnologia di riconoscimento facciale, sulla base di elementi fattuali ritenuti indicativi: da un lato, la straordinaria rapidità con cui è stata effettuata la sua identificazione, avvenuta nell'arco di meno di quarantotto ore dalla manifestazione; dall'altro, la tempestività con cui le forze di polizia sono riuscite a localizzarlo,

[174] C. eur., *Glukhin c. Russia*, cit., § 51.

[175] C. eur., *Glukhin c. Russia*, cit., § 60.

individuandone l'esatta posizione nel giro di meno di un'ora dall'uscita dalla sua abitazione [176].

Il caso in esame affronta una questione di rilevanza fondamentale, ovvero la possibilità per gli interessati di contestare l'impiego di tecnologie di riconoscimento facciale anche in assenza di una prova certa del loro effettivo utilizzo da parte delle autorità di *law enforcement*. In determinati contesti, secondo i giudici di Strasburgo, l'uso di software di riconoscimento facciale può essere ragionevolmente presunto sulla base di una serie di elementi oggettivi. In particolare, l'attenzione si è focalizzata sulla rapidità con cui è avvenuta l'identificazione dell'interessato, un elemento che, secondo i giudici, risulta difficilmente giustificabile in assenza dell'impiego di tecnologie biometriche avanzate.

Il ragionamento dei giudici passa poi a trattare la definizione di "vita privata", espressione dai confini ampi, in grado di includere molteplici aspetti dell'identità fisica e sociale di un individuo [177]. In particolare, l'attività di acquisizione e conservazione di informazioni concernenti la vita privata di un soggetto equivale già di per sé ad un'interferenza ai sensi dell'art. 8 della Convenzione europea. Pur sostenendo che l'ingerenza avesse una base giuridica di riferimento a livello nazionale [178], la Corte ha osservato come le disposizioni normative fossero state formulate in modo troppo ampio, senza la previsione di limitazioni, restrizioni o garanzie procedurali per gli interessati.

I giudici hanno dunque nuovamente eseguito un rigoroso scrutinio della conformità dell'impiego delle tecnologie di riconoscimento facciale alle condizioni di ammissibilità delle limitazioni al diritto alla vita privata, come sancito dall'art. 8. Tale verifica ha seguito il consolidato test tripartito, che impone l'accertamento della previsione della misura da parte della legge, della sua conformità agli scopi e della sua necessità in una società democratica.

Sotto il primo profilo, relativo alla base legale dell'ingerenza, la Corte ha individuato il fondamento normativo dell'impiego delle tecnologie di riconoscimento facciale nella disciplina nazionale russa, in particolare nel Codice di procedura amministrativa (CAO), nel Police Act e nel Decreto n. 410/2017, il quale autorizza l'installazione di telecamere con riconoscimento

---

[176] F. PALMIOTTO-N. MENENDEZ, *Facial recognition technology, democracy and human rights*, cit.

[177] C. eur., *Glukhin c. Russia*, cit., § 64.

[178] Code of Administrative Offences, Police Act, Decree no. 40.

facciale nella metropolitana di Mosca e ne consente l'accesso alle forze dell'ordine.

Tuttavia, la Corte ha rilevato che tale normativa nazionale non rispetta i requisiti di "qualità della legge", in quanto priva di norme dettagliate e di solide garanzie procedurali atte a prevenire il rischio di abusi e arbitrarietà[179]. In particolare, il legislatore russo non ha previsto disposizioni specifiche che disciplinino la portata e le modalità di impiego delle tecnologie di riconoscimento facciale, né ha introdotto meccanismi di supervisione indipendente o rimedi effettivi a tutela degli interessati. La Corte ha sottolineato che l'esigenza di salvaguardie adeguate risulta ancora più pregnante quando l'utilizzo di tali tecnologie avviene *in tempo reale*, poiché la loro invasività impone un livello elevato di protezione per i diritti fondamentali.

A rafforzare la conclusione sulla carenza qualitativa della normativa nazionale, i giudici hanno esaminato anche la disciplina russa sulla protezione dei dati personali (*Personal Data Protection Act* n. 152-FZ del 27 luglio 2006), evidenziando che essa consente il trattamento di dati biometrici senza il consenso dell'interessato per finalità di amministrazione della giustizia, attraverso una formulazione eccessivamente ampia e generica. Tale disposizione, priva di limiti stringenti in merito alle finalità di impiego, alle categorie di soggetti coinvolti e alla natura dei dati trattati, permette un utilizzo indiscriminato delle tecnologie di sorveglianza, senza prevedere meccanismi di autorizzazione, modalità di esame e conservazione dei dati, né strumenti di controllo indipendente.

Nel proseguire la propria analisi, i giudici hanno poi dato atto che l'uso delle tecnologie di riconoscimento facciale potrebbe astrattamente perseguire uno scopo legittimo, quale la prevenzione dei reati, in conformità all'art. 8, par. 2. Tuttavia, è stato chiarito che la valutazione della compatibilità con la Convenzione non può limitarsi a un esame astratto dell'ammissibilità dello strumento, bensì deve concentrarsi sul trattamento dei dati personali del singolo ricorrente nel caso concreto.

A questo punto, la Corte ha esaminato il terzo criterio del test di proporzionalità, interrogandosi sulla necessità dell'ingerenza in una società democratica. In tale prospettiva, ha sottolineato che l'impiego di tecnologie di riconoscimento facciale da parte delle autorità pubbliche rappresenta una forma di sorveglianza "altamente intrusiva", la cui legittimità richiede una giustificazione particolarmente rigorosa. I giudici hanno osservato che il

---

[179] Cfr. C. eur. 11 giugno 2020, *P.N. c. Germania*, § 56; C. eur. 13 febbraio 2020, *Gaughran c. Regno Unito*, § 96; C. eur. 11 giugno 2020, *P.N. c. Germania*, § 74.

ricorrente era stato evidentemente sottoposto a riconoscimento facciale per aver partecipato a una manifestazione pacifica e che l'unico illecito contestatogli era di natura amministrativa, senza che fosse stata integrata alcuna condotta effettivamente lesiva dell'ordine pubblico. Il ricorso a una tecnologia di sorveglianza così pervasiva per identificare e arrestare i partecipanti a un'azione di protesta pacifica è stato ritenuto idoneo a produrre un *chilling effect*, ovvero un effetto dissuasivo sulla libertà di espressione e di riunione.

Per tali ragioni, la Corte ha concluso che l'ingerenza non rispondesse a un bisogno sociale impellente e, pertanto, non soddisfacesse il requisito della necessità in una società democratica. Di conseguenza, ha accertato la violazione dell'art. 8, ritenendo l'utilizzo di tali tecnologie entro il contesto valutato incompatibile con gli ideali e i valori di una società democratica governata dallo Stato di diritto, che la Convenzione ha lo scopo di mantenere e promuovere.

L'avvertenza che arriva da Strasburgo è univoca e apre la via ad un filone esegetico consapevole e garantista. Benché la Corte riconosca che i software automatizzati di riconoscimento facciale possano rendere molto più efficienti alcune operazioni di ricerca e selezione di soggetti sospettati di reato da parte delle forze dell'ordine, i giudici sottolineano come «*the use of highly intrusive facial recognition technology in the context of the applicant exercising his Convention right to freedom of expression is incompatible with the ideals and values of a democratic society governed by the rule of law, which the Convention was designed to maintain and promote*» [180]. Dalla pronuncia è allora possibile desumere il principio fondamentale in base al quale le summenzionate misure di riconoscimento facciale dovrebbero essere impiegate solo se effettivamente giustificate da un obiettivo legittimo necessario, proporzionato e adeguatamente motivato.

Tuttavia, l'argomentazione sviluppata presenta diverse lacune sia sul piano esplicito delle affermazioni formulate, sia in relazione agli elementi implicitamente ammessi o omessi. Seppure i giudici si siano dichiarati espressamente intenzionati a mantenere il proprio giudizio aderente al caso specifico [181], evitando di pronunciarsi in via generale sulla legittimità delle

---

[180] C. eur., *Glukhin c. Russia*, cit., § 88.

[181] «*However, while it recognises the importance of such techniques in the detection and investigation of crime, the Court must delimit the scope of its examination. The question is not whether the processing of biometric personal data by facial recognition technology may in general be regarded as justified under the Convention. The only issue to be considered by the Court*

tecnologie di riconoscimento facciale, il percorso argomentativo adottato risulta eccessivamente generico e, di conseguenza, esposto al rischio di equivocità. La distinzione tra le modalità *a posteriori* e *in tempo reale* viene affrontata in modo superficiale, senza cogliere le implicazioni giuridiche e sistematiche che ne derivano. Sebbene sia possibile affermare che l'identificazione biometrica differita possa apparire, almeno in astratto, meno invasiva rispetto a quella effettuata *in tempo reale*, tale assunto non esaurisce la complessità del problema. Come autorevolmente sottolineato a livello europeo, l'impatto sulla tutela dei diritti fondamentali non dipende unicamente dal momento in cui avviene il trattamento dei dati biometrici, bensì dalla tecnologia adottata e dall'uso che ne viene fatto [182]. Un sistema di identificazione *in tempo reale* è infatti potenzialmente in grado di elaborare e conservare migliaia di profili in poche ore, con un effetto di controllo sociale diffuso e pervasivo che trascende la mera distinzione temporale tra riconoscimento *a posteriori* e *contestuale*. In quest'ottica, un'analisi più approfondita avrebbe dovuto prendere in considerazione le implicazioni sistemiche della tecnologia, alla luce delle politiche di sorveglianza adottate a livello nazionale e degli effettivi impieghi di tali strumenti da parte delle autorità di *law enforcement*. Al riguardo, sarebbe stato opportuno un maggiore approfondimento sull'esigenza di garantire standard più elevati di trasparenza nell'uso delle tecnologie di riconoscimento facciale, nonché la necessità di definire un chiaro regime di responsabilità per le violazioni dei diritti fondamentali derivanti da un impiego non adeguatamente regolamentato di tali strumenti.

In definitiva, l'approccio della Corte, pur rappresentando un'importante presa di posizione in merito alla tutela dei diritti fondamentali, appare ancora incompleto sotto diversi profili. Una maggiore attenzione alle caratteristiche intrinseche di questi strumenti, alla trasparenza dei processi decisionali e alle garanzie procedurali avrebbe consentito di meditare maggiormente su un quadro giuridico in grado di offrire un'effettiva protezione contro il rischio di abusi e arbitrarietà nel ricorso a questa tecnologia.

---

is whether the processing of the applicant's personal data was justified under Article 8 § 2 of the Convention in the present case». Cfr. C. eur., *Glukhin v. Russia*, cit., § 85.

[182] Cfr. EDPB & EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence* (Artificial Intelligence Act), 2021, § 31.

5. *I rischi per la parità delle armi*

Pur in assenza di una esplicita enunciazione nel testo dell'art. 6 Conv. eur. dir. uomo, il principio di parità delle armi è stato modellato dalla giurisprudenza della Corte di Strasburgo come pilastro fondamentale dell'equità processuale, al pari del diritto al contraddittorio [183]. Questa garanzia, squisitamente procedurale [184], interessa la «persona accusata di un reato» [185], intesa nel senso precisato dalla giurisprudenza della Corte di Strasburgo, secondo la quale un'ipotesi di accusa esiste «*from the moment that an individual is officially notified by the competent authority of an allegation that he has committed a criminal offence, or from the point at which his situation has been substantially affected by actions taken by the authorities as a result of a suspicion against him*» [186].

Con il *leading case Brandstetter c. Austria* [187], la Corte europea dei diritti dell'uomo ha ribadito un principio cardine del giusto processo, affermando che ogni parte deve avere piena e concreta conoscenza delle allegazioni e delle argomentazioni opposte, nonché la reale opportunità di contraddirle. Tale garanzia include il diritto dell'imputato di contestare gli elementi probatori prodotti dall'accusa, esercitando pienamente il proprio diritto di difesa attraverso la possibilità di confutare le risultanze istruttorie mediante la produzione di controprove. Una possibilità meramente teorica o indiretta di replicare alle argomentazioni dell'accusa non soddisfa gli standard richiesti dalla Convenzione [188].

---

[183] Cfr. M. CHIAVARIO, voce *Giusto processo (proc. pen.)*, in *Enc. giur.*, Treccani, Roma, 2001, p. 1; P. FERRUA, *Il giusto processo,* Zanichelli, Bologna, 2012, p. 1, parla di «modello ideale». Cfr. anche M. CHIAVARIO, *Diritto ad un processo equo*, in S. BARTOLE-B. CONFORTI, G. RAIMONDI (a cura di), *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, Cedam, Padova, 2001, p. 154 ss.

[184] Cfr. F. PALMIOTTO, *Black box on trial: the Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in M. EBERS-M. CANTERO GAMITO (a cura di), *Algorithmic Governance and Governance of Algorithms*, Springer, Berlin, 2020, p. 59.

[185] Art. 111, comma 3, Cost. Su questo punto cfr. M. CHIAVARIO, *Diritto ad un processo equo*, cit., p. 161 ss.

[186] In particolare C. eur. 27 febbraio 1980, *Deweer v. Belgium*, §§ 42-46, 6903/75; C. eur. 15 luglio1982, *Eckle v. Germany*, § 73, 8130/78; C. eur., *Ibrahim and Others v. the United Kingdom* [GC], no. 50541/08, 50571/08, 50573/08 e 40351/09, §249, 2016. Cfr. M. CHIAVARIO, *Diritto ad un processo equo*, cit., p. 162.

[187] Cfr. C. eur. 28 agosto 1991, *Brandstetter v. Austria*, § 68.

[188] C. eur., *Brandstetter v. Austria*, cit., § 68; C. eur. 10 marzo 1990, *Bykov v. Russia*, § 90.

Tuttavia, il principio di parità delle armi, così come delineato dalla giurisprudenza della Corte, non impone necessariamente un'assoluta simmetria tra le prerogative riconosciute alle parti processuali, né richiede un'identità perfetta di facoltà e posizioni giuridiche [189]. Piuttosto, esso si configura come un principio funzionale all'equità processuale, il cui obiettivo è quello di assicurare la possibilità di presentare le proprie argomentazioni in una condizione non svantaggiosa [190].

Alla luce di queste premesse di carattere generale, emergono alcune criticità connesse all'acquisizione e all'utilizzo di elementi di prova derivanti da processi automatizzati [191].

Si è fatto cenno alla capacità degli strumenti basati sull'apprendimento automatico (cd. *machine learning*), di costruire un proprio modello predittivo a partire dall'analisi dei dati con cui sono stati precedentemente addestrati [192]. La natura di tali sistemi rende però difficoltoso fornire una spiegazione del loro funzionamento intrinseco, ovvero delle motivazioni sottese a ciascun risultato raggiunto; questo perché il codice sorgente documenta esclusivamente le regole e i metodi utilizzati per elaborare i dati e costruire il modello, ma non è in grado di giustificare l'*output*, ossia una determinata previsione, classificazione o conclusione. La configurazione finale del modello, risultante dal processo di apprendimento e responsabile dei risultati del sistema, quindi, non è esplicitamente rappresentata nel codice [193].

Inoltre, quando il sistema è sviluppato da privati, l'accessibilità del codice sorgente può essere limitata per ragioni di proprietà intellettuale e dalla

---

[189] Cfr. P. VAN DIJK-G.J.H. VAN HOOF, *Theory and Practice of the European Convention on Human Rights*, V ed., Intersentia, Cambridge, 2018, p. 562 ss.

[190] Cfr. C. eur. 7 giugno 2001, *Kress c. Francia*, § 72.

[191] Per un approfondimento specifico sul tema, cfr. S. QUATTROCOLO, *Equo processo penale e sfide della società algoritmica*, cit., p. 138; ID., *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, 2020, p. 126 ss.;ID., *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Rev. Italo-espanola derecho procesal*, 1, 2019, p. 108 ss.; S. QUATTROCOLO-C. ANGLANO-M. CANONICO-M. GUAZZONE, *Technical Solutions for Legal Challenges: Equality of Arms in Criminal Proceedings*, in *Global Jurist*, 20(1), 2020, p. 6; C. CASONATO, *Intelligenza artificiale e giustizia: potenzialità e rischi*, in *DPCE Online*, 44(3), 2020, p. 3379 ss.; J. NIEVA FENOLL, *Intelligenza artificiale e processo*, trad. a cura di P. COMOGLIO, Giappichelli, Torino, 2019, p. 130.

[192] Cfr. il capitolo II, § 3.3.

[193] Cfr. M. HILDEBRANDT, *Algorithmic Regulation and the Rule of Law*, in *Phil. Trans. R. Soc*, 2018, p. 1-11.

necessità di proteggere i segreti commerciali e industriali [194]. Tale vincolo introduce significative implicazioni in termini di verificabilità dello strumento, poiché impedisce agli enti di controllo, alle autorità e alla comunità scientifica di esaminarne nel dettaglio il funzionamento, valutandone l'affidabilità e l'assenza di *bias* discriminatori.Questo contribuisce a rendere il comportamento del sistema e la spiegazione delle sue decisioni molto complessi da interpretare: si parla a tal proposito di "*black boxes*", cioè sistemi in cui *input* e *output* sono osservabili, mentre il funzionamento interno rimane oscuro anche agli stessi programmatori dello strumento [195].

L'opacità dei meccanismi di funzionamento interni agli strumenti di intelligenza artificiale assume particolare rilevanza per i sistemi di riconoscimento facciale, ove il modello che coinvolge il confronto e la verifica dei volti si basa su rappresentazioni automatiche e su una moltitudine di parametri che risultano difficilmente decifrabili. Per poter contestare efficacemente un risultato di compatibilità, è necessario che il soggetto interessato abbia accesso a tutte le informazioni rilevanti, in particolare ai *dataset* (insiemi di dati), ai metodi di trattamento dei dati, e al codice sorgente che descrive i modelli alla base del funzionamento del sistema.

Il quesito centrale riguarda qui l'effettiva verificabilità dei processi algoritmici, ossia la capacità per la difesa di comprendere, analizzare e, se del caso, confutare i risultati prodotti dagli strumenti tecnologici utilizzati dall'accusa. Emerge il rischio di una disparità strutturale di conoscenze e risorse tra le parti del processo, configurando un disequilibrio conoscitivo che potrebbe compromettere l'effettività del diritto di difesa. L'accusa, in virtù del suo accesso privilegiato alle più avanzate tecnologie di analisi e identificazione, nonché della disponibilità di risorse economiche e istituzionali più ampie, si trova in una posizione di vantaggio oggettivo rispetto alla parte privata, la quale potrebbe non disporre di mezzi tecnici adeguati o di competenze specialistiche per sottoporre a scrutinio critico i risultati generati dai software impiegati nel procedimento.

Questa asimmetria conoscitiva non è nuova nel panorama processuale,

---

[194] Cfr. J.A. SEAMAN, *Black Boxes*, in *Emory Law Journal,* 58(2), 2008, p. 427-488.

[195] Cfr. F. PASQUALE, *The black box society: The secret algorithms that control money and information*, Harvard University Press, London, 2015. Si dà conto che secondo alcuni ricercatori sarebbe possibile fornire un modello interpretabile e trasparente che sia in grado di replicare il processo decisionale della *black box*, rendendolo intellegibile. Cfr. *ex multis* R. GUIDOTTI-A. MONREALE-S. RUGGIERI-F. TURINI-D. GIANNOTTI-F. PEDRESCHI, *A survey of methods for explaining black box models*, in *ACM Comput. Surv.*, 51(5), 2018, 93:1-93:42.

ma si inserisce in un fenomeno più ampio relativo all'introduzione di saperi specialistici nel giudizio penale, laddove la parte pubblica, avvalendosi di consulenti tecnici e di strumenti di investigazione scientifica avanzata, gode di un accesso privilegiato a strumenti di analisi altamente sofisticati. Tuttavia, «la prova algoritmica (…) introduce la forma più estrema di tale squilibrio, poiché il risultato probatorio può essere non criticabile laddove, appunto, l'inaccessibilità del codice sorgente o altre caratteristiche del software non consentano alla parte contro la quale la prova è introdotta nel processo di contestarne l'accuratezza e l'attendibilità» [196].

Volendo indagare la questione rispetto alle più specifiche categorie di dati "*trasformati/convertiti*", "*ricavati*" e "*generati automaticamente*" [197], occorre applicare alcune distinzioni. Nei primi due casi, il procedimento di riconoscimento biometrico, pur avvalendosi di strumenti algoritmici avanzati, non si traduce in un'esclusiva elaborazione automatizzata del dato, poiché il risultato prodotto dal software rimane "parziale" e privo di una quantificazione automatica del rapporto di verosimiglianza. Quest'ultimo, come già visto, costituisce un parametro essenziale per valutare il grado di affidabilità dell'identificazione ed è oggetto di una successiva analisi e validazione da parte di esperti umani, che operano in base a standard metodologici codificati. In questa prospettiva, il ruolo dell'operatore specializzato si configura come «una salvaguardia di importanza fondamentale» [198]: l'intervento umano costituisce una garanzia mitigando, seppure non eliminando del tutto, il rischio di decisioni algoritmiche errate che potrebbero condizionare in modo irreversibile l'accertamento della verità processuale.

Non sembra possibile trarre le medesime conclusioni rispetto ai *matches* generati automaticamente da strumenti di uso generico o commerciale, quali assistenti domestici o dispositivi elettronici di rilevamento delle proprie caratteristiche fisiologiche o comportamentali. In questi casi, il dato non è il

---

[196] Cfr. S. QUATTROCOLO, *Equo processo penale e sfide della società algoritmica*, cit., p. 139.

[197] Come visto, a seconda della tecnologia impiegata e dello scopo del trattamento, il dato biometrico può assumere la forma di un *template* digitalizzato, essere estratto da supporti video oppure essere generato da dispositivi automatizzati d'uso quotidiano. Cfr. il capitolo II, § 5.

[198] Cfr. J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del garante privacy d'oltremanica)*, in *Sist. pen.*, 28 marzo 2020, p. 235.

risultato di un'elaborazione progressiva e verificabile successivamente da parte di un esperto in base a standard univoci, ma deriva da un confronto 1:1, eseguito in modo automatico dagli algoritmi del software, che opera secondo logiche proprietarie né trasparenti né accessibili. Il procedimento di riconoscimento in questo caso implica che una volta registrati, i dati siano elaborati e le conclusioni siano tratte integralmente dal software. Il rischio principale è che il risultato, non potendo tecnicamente essere oggetto di un successivo scrutinio umano indipendente [199], venga accettato come una verità preconfezionata, difficilmente contestabile per l'assenza di documentazione metodologica e di parametri tecnici chiari su cui fondare eventuali eccezioni. Risalire alla rappresentazione digitalizzata del dato biometrico registrato risulta tecnicamente molto complesso quando non impossibile, precludendo la possibilità di integrare successivamente il procedimento di riconoscimento con l'intervento umano. I risultati non si basano su linee guida o protocolli sicuri, né sono necessariamente concepiti con l'obiettivo specifico di essere impiegati per scopi giudiziari. Se il nucleo essenziale dell'equità processuale risiede nel diritto della difesa di contestare l'ammissibilità e l'affidabilità delle prove a carico, allora l'impossibilità di verificare *ex post* l'*output* di un algoritmo potrebbe configurare, in sé, una violazione dell'art. 6 Conv. eur. dir. uomo [200].

Il nodo cruciale della questione diviene allora la necessità di verificare la sussistenza di strumenti tecnici e processuali idonei a garantire alla difesa un accesso effettivo e consapevole ai criteri di formazione della prova algoritmica. In un sistema processuale improntato ai principi di contraddittorio e parità delle armi, la possibilità per la parte indagata o imputata di comprendere i meccanismi sottesi alla generazione dell'*output* costituisce il presupposto imprescindibile per un esercizio effettivo e non meramente formale del diritto di difesa.

---

[199] La non riproducibilità del risultato e l'indecifrabilità dei processi interni al modello di riconoscimento rendono problematico ogni tentativo di ricostruzione a ritroso. L'assenza di spiegabilità impedisce di comprendere come si sia giunti al risultato. Cfr. il capitolo III, § 4.1.

[200] Cfr. S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, Springer, Cham, 2020, p. 74 ss.

5.1. *I sistemi di intelligenza artificiale tra trasparenza e spiegabilità dei risultati: i rimedi tecnici indispensabili al diritto di difesa e al contraddittorio*

Al di là della specifica complessità legata al riconoscimento facciale, sono stati elaborati diversi indirizzi validi per regolare l'impiego degli strumenti di IA, che hanno la funzione di stabilire alcuni limiti per un loro uso "etico". Tali criteri si propongono di orientare lo sviluppo, l'implementazione e l'uso dell'intelligenza artificiale, assicurando che questi strumenti siano impiegati nel rispetto dei diritti fondamentali, della dignità umana e dei principi di equità e non discriminazione.

I principi sono stati formalizzati attraverso una pluralità di strumenti normativi e regolatori con l'obiettivo di stabilire un quadro di riferimento per lo sviluppo e l'impiego responsabile dell'intelligenza artificiale. A partire dalle *Ethics Guidelines for trustworthy AI* del gruppo di esperti ad alto livello sull'intelligenza artificiale istituito dalla Commissione europea nel giugno 2018[201], alla *Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia* emanata nell'ambito del Consiglio d'Europa nel dicembre 2018[202], fino al *regolamento sull'intelligenza artificiale*[203].

L'interazione tra principi etici, documenti di *soft law* e normative cogenti di *hard law* evidenzia il progressivo consolidarsi di un approccio multilivello, volto a garantire un utilizzo dell'intelligenza artificiale compatibile con i principi dello Stato di diritto e della protezione dei diritti fondamentali, attraverso un bilanciamento tra innovazione tecnologica e salvaguardia delle libertà individuali.

Il principio di *trasparenza tecnica* costituisce il fondamento essenziale del quadro normativo e tecnologico di riferimento per l'adozione e l'impiego dei sistemi di intelligenza artificiale e riconoscimento biometrico. Tale principio si articola su due livelli: da un lato, la trasparenza del codice sorgente del

---

[201] Il documento è reperibile all'indirizzo https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai-. Da qui in avanti anche "*Carta etica*" o "*Carta etica europea*".

[202] CEPEJ – *European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment*, reperibile su https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment

[203] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024. Per l'analisi del regolamento, si rinvia integralmente al capitolo IV, § 3.2.

sistema algoritmico, che consente di apprezzare le caratteristiche tecniche interne al medesimo [204]; dall'altro, la documentazione tecnica di accompagnamento, che deve contenere informazioni chiare e dettagliate sulla metodologia utilizzata, sulle logiche decisionali sottostanti e sulle modalità di impiego del sistema [205].

La trasparenza è stata elevata a rango di nuova e ulteriore garanzia del sistema a partire già dal regolamento (UE) 2016/679 sulla protezione dei dati

---

[204] Il tema dell'accesso alle modalità di funzionamento di un determinato algoritmo ha fatto il suo debutto in Italia nell'ambito della giurisprudenza amministrativa (cfr. Cons. Stato, sez. VI, 8 aprile 2019, n. 2270). Il supremo Consesso ha fissato alcuni principi che rendono legittimo il provvedimento integralmente automatizzato, tra i quali quello della conoscibilità del meccanismo che presiede la decisione automatizzata «secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico» e che si estende agli autori, al procedimento utilizzato per la sua elaborazione, al meccanismo decisionale, comprensivo della procedura valutativa e decisionale dei dati selezionati come rilevanti, e quello dell'assoggettamento alla piena cognizione del giudice amministrativo, il quale deve essere posto in grado di poter sindacare la logicità e la ragionevolezza della regola che governa l'algoritmo. In precedenza, il TAR Lazio, sez. III-*bis*, 10 settembre 2018, n. 9227 ha affermato che «alcuna complicatezza o ampiezza, in termini di numero di soggetti coinvolti ed ambiti territoriali interessati, di una procedura amministrativa, può legittimare la sua devoluzione ad un meccanismo informatico o matematico del tutto impersonale e orfano di capacità valutazionali delle singole fattispecie concrete, tipiche invece della tradizionale e garantistica istruttoria procedimentale che deve informare l'attività amministrativa, specie ove sfociante in atti provvedimentali incisivi di posizioni giuridiche soggettive di soggetti privati e di consequenziali ovvie ricadute anche sugli apparati e gli assetti della pubblica amministrazione». Per un commento sulla decisione, cfr. M. CATANZARITI, *Enhancing Policing through Algorithmic Surveillance*, cit., p. 253.

[205] Cfr. M. EBERS, *Regulating AI and Robotics: Ethical and Legal Challenges*, in M. EBERS-S.N. NAVARRO (eds.), *Algorithms and Law*, Cambridge University Press, Cambridge, 2019, p. 12 «*we can see only input data and output data for algorithm-based systems without understanding exactly what happens in between*»; J.A. KROLL-J. HUEY-S. BAROCAS-E.W. FELTEN-J.R. REIDENBERG-D.G. ROBINSON-H. YU, *Accountable Algorithms*, in *U. Pa. L. Rev.*, 633, 2017; A.M. CRAWFORD, *Seeing without knowing: limitations of the transparency ideal and its application to algorithmic accountability*, in *New Media Soc*, 2018, 20:973; P. PERRI, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè, Milano, 2020, p. 134; F. PALMIOTTO, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in M. EBERS-M. CANTERO GAMITO (eds.), *Algorithmic Governance and Governance of Algorithms, Legal and Ethical Challenges*, Springer, Berlin, 2020, p. 56 ss. e F. PALMIOTTO, *The Right to Contest Automated Decisions*, 14 febbraio 2022, reperibile all'indirizzo https://digi-con.org/the-right-to-contest-automated-decisions/.

personali che, in diverse parti [206], richiama il requisito con riferimento alle modalità di trattamento con cui sono «raccolti, utilizzati, consultati o altrimenti trattati dati personali […] nonché la misura in cui i dati personali sono o saranno trattati» [207]. Le informazioni e le comunicazioni relative alla gestione dei dati personali devono essere facilmente accessibili e comprensibili e deve essere utilizzato un linguaggio semplice e chiaro. Ne consegue una logica applicazione anche a scenari dominati da strumenti che si servono di tecniche automatizzate, interessati da un sistematico utilizzo di dati personali.

Con la *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi* [208], viene richiamato il rispetto del principio in esame, ponendolo in stretto collegamento con l'imparzialità e la *fairness* (art. 4): in particolare, la Carta raccomanda l'accessibilità, la comprensibilità e la verificabilità esterna dei processi computazionali utilizzati per l'analisi dei dati giudiziari. Pertanto non è sufficiente l'accesso alle caratteristiche tecniche dello strumento ma occorre garantire anche la cd. "spiegabilità" del processo computazionale in un linguaggio accessibile e chiaro [209]. Mentre la trasparenza implica la possibilità di avere accesso a tutti gli elementi tecnici del software in uso, la "spiegabilità" consiste in una descrizione del procedimento mediante il quale un decisore, considerando un insieme di dati di *input*, ha raggiunto una determinata conclusione [210].

Anche il regolamento sull'intelligenza artificiale conferma il necessario rispetto della trasparenza [211], intesa come insieme di informazioni sul sistema di IA: a seconda del livello di "rischio" associato all'utilizzo di un determinato strumento è prevista una corrispondente "classe" di trasparenza

---

[206] Cfr. i considerando 39, 58, 60, 71, 78, 100 e 121, e il requisito viene menzionato agli artt. 5, 12, 13, 53 e 88.

[207] Cfr. il considerando 39, cit.

[208] Cfr. https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348.

[209] Cfr. S. QUATTROCOLO, *Intelligenza artificiale e giustizia nella cornice della Carta etica europea. Gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *Leg. pen.*, 18 dicembre 2018.

[210] Trattasi di due principi distinti ma strettamente correlati. Cfr. F. PALMIOTTO, *The Right to Contest Automated Decisions*, 14 febbraio 2022, cit. e B. WALTL-R. VOGL, *Explainable Artificial Intelligence – the New Frontier in Legal Informatics*, in *Jusletter* IT, 22 febbraio 2018.

[211] Art. 13.

algoritmica. Per i sistemi classificati a "basso rischio", vengono introdotti requisiti minimi di trasparenza, volti a garantire che l'utente sia consapevole dell'interazione con uno strumento di intelligenza artificiale e che sia fornita una documentazione di base sulle modalità di funzionamento dello stesso. Diversamente, per i sistemi ad "alto rischio", il rispetto del principio di trasparenza diviene un requisito imprescindibile ai fini della loro legittima implementazione e utilizzo. In particolare, l'art. 13 del regolamento stabilisce che tali sistemi devono essere progettati e sviluppati in modo da assicurare un livello di trasparenza sufficiente affinché gli utenti possano comprendere, interpretare e utilizzare in modo appropriato l'*output g*enerato dal modello.

A sua volta, l'art. 86 introduce poi il diritto alla "spiegazione" di una decisione adottata sulla base dell'*output* di un sistema di IA ad alto rischio. Più precisamente, la disposizione sancisce il diritto di ottenere dal *deployer*[212] spiegazioni chiare e significative in merito al ruolo svolto dal sistema di IA nel processo decisionale, nonché ai principali elementi che hanno contribuito alla decisione adottata. La norma non fa riferimento alla "*feature salience*", intesa come spiegabilità delle caratteristiche o variabili più influenti nei dati di *input* che determinano l'intero processo decisionale. Analogamente, non viene menzionato il concetto di "*counterfactual explanations*", che descrive le motivazioni secondo cui una lieve variazione nei dati di ingresso potrebbe condurre a un esito decisionale diverso[213]. L'assenza di tali riferimenti limita la possibilità di stabilire un quadro esplicativo più approfondito e strutturato, essenziale per comprendere in modo analitico le dinamiche interne di questi sistemi e, conseguentemente, per rafforzare la fiducia e la responsabilità nei confronti delle decisioni automatizzate[214].

---

[212] Definito come «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale». Art. 3, par. 1, n. 4.

[213] Cfr. P. HACKER, *Comments on the Final Trilogue Version of the AI Act*, reperibile all'indirizzo https://www.europeannewschool.eu/images/chairs/hacker/Comments%20on%20the%20AI%20Act.pdf.

[214] Per un approfondimento sul tema si rinvia a M.E. KAMINSKI-G. MALGIERI, *The Right to Explanation in the AI Act*, in *U of Colorado Law Legal Studies Research Paper*, No. 25-9, 2025.

5.2. *Tra interpretabilità e certificazione del metodo*

Sebbene non sia stata ancora definita da un punto di vista normativo [215], strettamente connessa ai principi di trasparenza e spiegabilità degli strumenti è l'*interpretabilità* [216]. L'effettiva trasparenza di un sistema algoritmico dipende dalla precisione della teoria scientifica che la sostiene e, in secondo luogo, dalla chiarezza del linguaggio utilizzato per tradurlo in un modello matematico [217]. Da un punto di vista informatico, infatti, un linguaggio matematico chiaro permette ad un operatore di comprendere *ex post* il procedimento che, da un dato *input*, ha portato ad un determinato *output* [218]. Da qui, parte della letteratura definisce l'*interpretabilità* come «*the degree to which a human can understand the cause of a decision*» [219], altra parte invece come «*the degree to which a human can consistently predict the model's result*» [220]. In questo senso, si pone come un *trait d'union* fra la "trasparenza" e la "spiegabilità", richiedendo che un sistema di IA possa definirsi come una *white box*, o cd. "scatola di vetro", attraverso l'analisi del modello logico di apprendimento alla base del sistema considerato.

La spiegabilità, alla luce di questo ulteriore passaggio, assume un significato più ampio, riferendosi ad una serie di caratteristiche che rendono un sistema di intelligenza artificiale altamente comprensibile ai destinatari, tra cui la descrizione del procedimento che pone tutte le informazioni del

---

[215] Anche in letteratura si registra una certa sovrapposizione concettuale tra le espressioni "*transparency*", "*explainability*" e "*interpretability*". Cfr. F. PALMIOTTO, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in M. EBERS-M. CANTERO GAMITO (eds.), *Algorithmic Governance and Governance of Algorithms, Legal and Ethical Challenges*, cit., p. 56 ss.; G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., p. 212 ss.

[216] La nozione di "interpretabilità" non è stata ancora univocamente definita in letteratura. Su questo punto, cfr. Z.C., LIPTON, *The mythos of model interpretability*, in *arXiv*, 2016.

[217] Cfr. C. VILLANI, *AI for Humanity–French National Strategy for Artificial intelligence*, 2018, reperibile all'indirizzo https://www.aiforhumanity.fr/en/ e A.K. JAIN-D. DEB-J.J. ENGELSMA, *Biometrics: Trust, but Verify*, cit., p. 10.

[218] Cfr. V. CARVALHO-E. M. PEREIRA-J. S. CARDOSO, *Machine Learning Interpretability: A Survey on Methods and Metrics*, in *Electronics*, 2019, 8, p. 832.

[219] Cfr. T. MILLER, *Explanation in Artificial Intelligence: Insights from the social sciences*, in *Artif. Intell.*, 2018, 267, p. 1 ss.

[220] Cfr. B. KIM-R. KHANNA-O.O. KOYEJO, *Examples are not enough, learn to criticize! Criticism for interpretability*, in *Advances in Neural Information Processing Systems*, The MIT Press, Cambridge, 2016, p. 2280 ss.

sistema direttamente accessibili agli utenti. Tra IA *spiegabile* e IA *interpretabile* la finalità rimane la stessa, ossia la trasparenza "rafforzata" dell'algoritmo posto alla base del funzionamento di un sistema.

V'è da rilevare che, nell'ambito delle scienze forensi, le ricerche più avanzate non si concentrano tanto sulla spiegabilità del risultato (ritenuta soltanto desiderabile), quanto piuttosto sull'analisi delle condizioni operative in cui il metodo viene applicato e, in taluni casi, fallisce [221]. Questo approccio riflette una prospettiva pragmatica, orientata a comprendere non solo l'efficienza del sistema in scenari ideali, ma anche la sua "resilienza" in contesti complessi, caratterizzati da variabili non controllate e da condizioni operative eterogenee. La ripetizione di test in ambienti non standardizzati e in condizioni operative diversificate contribuisce, infatti, ad accrescere il grado di fiducia nei confronti del metodo, poiché consente di delinearne con maggiore precisione i limiti e le potenzialità. In questo senso, la validazione non si esaurirebbe in una mera certificazione di conformità tecnica, ma diventerebbe un processo continuo di verifica empirica e di affinamento delle capacità predittive del sistema. La ripetibilità, intesa come la capacità di ottenere risultati coerenti e replicabili in condizioni analoghe, rappresenta infatti uno dei pilastri fondamentali del metodo scientifico e una garanzia imprescindibile per la legittimità dell'utilizzo di tali tecnologie in ambito forense e processuale.

Pertanto, secondo questo filone interpretativo, nell'impossibilità di spiegare il funzionamento interno del modello di IA – ossia dell'"intelligibilità" del processo decisionale automatizzato – sarebbe più opportuno spostare il focus sull'affidabilità empirica del metodo [222]. In quest'ottica, la questione centrale non sarebbe tanto quella di comprendere come l'algoritmo giunga a un determinato esito, quanto quella di valutare in che misura tale esito sia stato sottoposto a rigorosi processi di verifica e validazione scientifica. Ciò implica la necessità di testare il sistema attraverso una serie controllata di esperimenti, condotti in condizioni variabili e documentate, al fine di consolidare un quadro probatorio robusto e verificabile.

---

[221] «The question is whether explainability is merely desiderable, or a necessity». Y.D. RAMOS-D. MEUWLY, *AI-based Forensic Evaluation in Court: The Desiderability of Explanation and the Necessity of Validation*, in Z. GERADTS-K. FRANKE (eds.), *Artificial Intelligence (AI) in Forensic Sciences*, John Wiley & Sons Inc, Hoboken, 2023, p. 7.

[222] «(…) *particularly for systems that are too complex to fully understand, validation is a necessity as it allows us to make informed decisions on if and when to apply them*». Y.D. RAMOS-D. MEUWLY, *AI-based Forensic Evaluation in Court: The Desiderability of Explanation and the Necessity of Validation*, cit., p. 8.

5.3. *I criteri di equità e di legalità*

Ulteriore principio etico richiamato nei tre documenti è la *fairness.* Con le *Ethics Guidelines for trustworthy AI*, il principio di equità è stato inteso in senso sia sostanziale sia processuale. Il primo implica un impegno a garantire una distribuzione giusta ed equa di costi e di benefici e ad assicurare che gli individui e i gruppi siano liberi da distorsioni inique, discriminazioni e stigmatizzazioni. La dimensione procedurale del principio di equità si sostanzia nella necessità di garantire un effettivo diritto di contestazione e impugnazione delle decisioni adottate mediante sistemi di IA, nonché di quelle assunte direttamente dagli esseri umani. Ciò implica che ogni processo decisionale, indipendentemente dal fatto che sia interamente automatizzato o frutto di un'interazione tra tecnologia e attività umana, debba essere trasparente e verificabile.

Con la *Carta etica europea*, si ribadisce con enfasi uno stretto collegamento logico tra *fairness, imparzialità e trasparenza:* in particolare, si raccomanda l'accessibilità, la comprensibilità e la verificabilità esterna dei processi computazionali utilizzati per l'analisi dei dati giudiziari. Nel bilanciamento fra l'interesse di assicurare la giustizia e quello privato dello sviluppatore del software deve prevalere il primo [223], e questo può avvenire solo se tutto il ciclo di progettazione, sviluppo e utilizzo del modello è ispirato ai tre requisiti richiamati. Il documento su questo punto non si espone ulteriormente, lasciando alle autorità dei diversi Stati membri la possibilità di cogliere e modellare il suggerimento in base alle caratteristiche di ciascun ordinamento [224].

In tutti e tre i documenti, poi, si fa cenno al generale principio di legalità (*lawfulness*). Nella nota esplicativa della Carta etica si evidenzia come gli strumenti di IA debbano essere progettati seguendo un generale approccio di protezione dai potenziali rischi di violazione dei diritti fondamentali (*human-rights-by-design*) che, nell'ambito dell'amministrazione della giustizia, attengono al diritto di accesso alla giurisdizione, al diritto ad un processo equo, alla parità delle armi, al principio di legalità, alla libertà personale/morale etc. [225].

---

[223] Cfr. S. QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea*, cit.

[224] Cfr. S. QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea*, cit.

[225] Cfr. S. QUATTROCOLO, *Intelligenza artificiale e giustizia nella cornice della Carta etica europea*, cit.

Nel quadro normativo ed etico delineato dalle disposizioni finora esaminate, il principio di non discriminazione emerge come un fondamento imprescindibile nella regolamentazione dell'intelligenza artificiale (IA). Tale principio viene reiterato in più occasioni, stabilendo il divieto assoluto di impiegare strumenti basati su IA per generare, legittimare o aggravare disparità di trattamento tra gruppi sociali e individui. Nel suo impiego, infatti, l'idea che l'IA possa eliminare o addirittura ridurre gli errori o i pregiudizi che possono condizionare l'esito del procedimento è stata da tempo ritenuta infondata [226]. Gli errori e i pregiudizi già insiti nel pensiero umano possono riprodursi ed essere perfino amplificati dalle tecniche di IA [227]. Il pericolo di ottenere risultati discriminatori può verificarsi a più livelli [228]: l'*input*, non risultando sempre completamente neutro, potrebbe influenzare l'*output*, generando la discriminazione di singoli individui o di interi gruppi sociali [229]; inoltre, la deriva discriminatoria potrebbe manifestarsi con la riproduzione di ingiustificati pregiudizi sociali [230]. Pertanto, sia i soggetti pubblici sia quelli privati devono garantire che gli strumenti non conducano ad analisi discriminatorie, a maggior ragione quando si considerino dati sensibili, quali quelli relativi all'origine razziale o etnica, al *background* socio-economico, alle opinioni politiche, ai dati genetici o biometrici.

L'analisi dei tre documenti evidenzia una convergenza sostanziale tra le istituzioni europee e internazionali nel perseguire l'obiettivo comune di costruzione di una regolamentazione etica e giuridicamente solida dell'intelligenza artificiale, segno di una consapevolezza della necessità di un approccio normativo uniforme e trasversale. Le numerose e recenti iniziative legislative testimoniano una svolta epocale nel rapporto tra tecnologia e diritto, caratterizzata da un continuo e delicato bilanciamento tra innovazione e tutela dei diritti fondamentali, nel tentativo di armonizzare il progresso scientifico con il rispetto delle libertà individuali. La scelta delle

---

[226] Cfr. F. PASQUALE, *The Black Box Society: The Secret Algorithms that Control Money and Information*, cit., p. 102 ss. e F. DONATI, *Intelligenza artificiale e giustizia*, in *Riv. AIC*, 1, 2 marzo 2020, p. 421.

[227] Cfr. M. EBERS, *Regulating AI and Robotics: Ethical and Legal Challenges,* cit., p. 33.

[228] Cfr. Appendice esplicativa alla Carta etica europea, reperibile su https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348

[229] Cfr. S. QUATTROCOLO, *Intelligenza artificiale e giustizia nella cornice della Carta etica europea*, cit.

[230] Su questo punto la letteratura risulta assai ricca, v. *ex multis* T.P. WOODS, *The Implicit Bias of the Implicit Bias Theory*, in *Dr. L. Rev.*, 2017, p. 631 ss.

istituzioni sovranazionali di reinterpretare le garanzie giuridiche tradizionali alla luce delle nuove sfide poste dall'intelligenza artificiale appare oggi l'unica strategia percorribile per verificare l'effettività del diritto positivo vigente, assicurando che le norme esistenti siano in grado di rispondere alle trasformazioni profonde e sistemiche che l'IA sta introducendo nella società. Questa operazione di rilettura critica del quadro normativo consente non solo di valutare l'adeguatezza degli strumenti giuridici già in vigore, ma anche di sviluppare un diritto tecnologicamente consapevole, in grado di governare e non subire l'innovazione. In questo scenario, la regolamentazione dell'intelligenza artificiale si configura come un processo dinamico e adattivo, che richiede una costante revisione dei principi cardine del diritto, in modo da assicurare che le garanzie fondamentali non vengano erose dal progresso tecnologico, ma piuttosto rafforzate e ridefinite in sua funzione. La sfida normativa non consiste, dunque, nella mera introduzione di vincoli formali, ma nella costruzione di un modello giuridico capace di coniugare l'efficienza tecnologica con il rispetto dei valori costituzionali, garantendo che il diritto rimanga uno strumento di tutela e non di ostacolo allo sviluppo scientifico [231].

[231] Cfr. il capitolo VI, § 1.

Capitolo IV

Tentativi di regolamentazione fra normativa interna e sovranazionale

SOMMARIO: 1. Considerazioni introduttive. – 2. L'esperienza italiana e il SARI. – 2.1. Il decreto "capienze" e l'inerzia del legislatore. – 3. Il quadro normativo sovranazionale: verso un sistema armonizzato di regole. – 3.1. Dal Libro bianco della Commissione europea alla Convenzione sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto nell'ambito del Consiglio d'Europa. – 3.2. Il regolamento europeo sull'intelligenza artificiale. – 3.2.1. I sistemi di riconoscimento biometrico a distanza: per la prima volta uno schema normativo di riferimento. – 3.2.2. Gli strumenti di riconoscimento *in tempo reale*. – 3.2.3. Gli strumenti di riconoscimento *a posteriori*. – 3.2.4. Alcune prime brevi riflessioni sul regolamento. – 4. Le ricadute sulla cooperazione di polizia e gli sviluppi del sistema di scambio e di circolazione dei dati.

1. *Considerazioni introduttive*

Accertati i potenziali rischi che l'impiego di tecnologie di riconoscimento facciale comporta per la tenuta di garanzie processuali fondamentali, si impone ora un'analisi sistematica della disciplina normativa vigente, volta a regolamentarne l'utilizzo e ad attenuarne le criticità applicative.

Il primo dato da rilevare è che, sia a livello europeo sia a livello nazionale, sono state recentemente adottate disposizioni destinate a regolare l'impiego di questi strumenti, compiendo così un importante passo verso una *governance* consapevole di questa tecnologia [1].

Sul piano interno, si osserva, da una parte, la presenza di alcune disposizioni settoriali e non necessariamente coordinate, che concorrono a definire il quadro normativo sulle condizioni di utilizzo e i possibili impieghi di queste tecnologie. Per esempio, con l'art. 5 *septies* del d.l. 18 aprile 2019, n. 32

[1] Cfr. il capitolo I, § 3.

(cd. "sblocca cantieri"), convertito con legge 14 giugno 2019, n. 55, è stato stanziato un fondo di venti milioni di euro «finalizzato all'erogazione a favore di ciascun comune delle risorse finanziarie occorrenti per l'installazione di sistemi di videosorveglianza a circuito chiuso presso ogni aula di ciascuna scuola nonché per l'acquisto delle apparecchiature finalizzate alla conservazione delle immagini»[2]. Inoltre, si pensi a quelle fonti che, nell'ambito delle misure tese a incrementare la sicurezza urbana, autorizzano gli enti territoriali a ricorrere a sistemi di videosorveglianza[3], compreso l'uso di strumenti «tecnologicamente avanzati, dotati di software di analisi video per il monitoraggio attivo»[4].

Se è vero che la normativa di settore affonda le proprie radici nel più ampio contesto della legislazione nazionale sulla tutela dei dati personali, quest'ultima si profila, nello scenario italiano, come unico sfondo legislativo rilevante. Tuttavia, come si è visto, essa si configura – in virtù della sua ampia portata normativa – come uno strumento capace non solo di affrontare alcune delle questioni più complesse e controverse sollevate dall'impiego di tali tecnologie, ma anche di individuare, in modo sistematico, le eventuali limitazioni che queste possono imporre ad altri diritti fondamentali[5]. Per questa ragione, l'analisi sulla normativa interna prenderà avvio proprio dai provvedimenti emessi, su tale base, dall'Autorità nazionale garante per la

---

[2] Il comma 2 della medesima disposizione destina un importo analogo per l'installazione degli stessi dispositivi presso strutture socio-sanitarie e socio-assistenziali per anziani e persone con disabilità.

[3] Per es. il d.l. 23 febbraio 2009, n. 11, recante "*Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori*", convertito con legge 23 aprile 2009, n. 38, che all'art. 6, commi 7 e 8, prevede l'utilizzabilità, da parte dei Comuni, di sistemi di videosorveglianza in luoghi pubblici.

[4] Cfr. il d.l. 20 febbraio 2017, n. 14, convertito con modificazioni con la legge 18 aprile 2017, n. 48, che istituisce i c.d. "Patti per l'attuazione della sicurezza urbana", tra il prefetto ed il sindaco, attraverso cui individuare interventi sulla sicurezza urbana, per obiettivi, tra l'altro, quali prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria anche «attraverso l'installazione di sistemi di videosorveglianza» (art. 5, comma 2, lett. a). Nell'ambito di tali patti, oltre che degli accordi conclusi tra Stato e Regioni per la promozione della sicurezza integrata ai sensi dell'art. 3, possono essere individuati specifici obiettivi per l'incremento dei servizi di controllo del territorio e per la sua valorizzazione, comprensivi anche di progetti «per la messa in opera a carico di privati di sistemi di sorveglianza tecnologicamente avanzati, dotati di software di analisi video per il monitoraggio attivo con invio di allarmi automatici a centrali delle forze di polizia o di istituti di vigilanza privata convenzionati» (art. 7, comma 1-*bis*).

[5] Cfr. il capitolo III.

protezione dei dati personali, in relazione agli impieghi della tecnologia di riconoscimento facciale, nel più specifico ambito di *law enforcement*, per poi articolarsi in una disamina approfondita delle disposizioni specificamente introdotte a livello interno per la regolamentazione. Tale panoramica è finalizzata a valutare l'efficacia delle norme in esame, a partire dalla necessità di soddisfare i requisiti posti dalla riserva di legge e di giurisdizione a tutela di alcune garanzie fondamentali richiamate nel precedente capitolo (in particolare dagli artt. 2, 13 Cost., 8 Cedu, 7 e 8 CDFUE), nonché individuarne eventuali limiti intrinseci. Particolare attenzione sarà rivolta poi alle eventuali criticità applicative che potrebbero emergere nella fase empirica di applicazione e alle potenziali lacune per la tutela dei diritti fondamentali.

La disciplina sulla tecnologia di riconoscimento biometrico in ambito europeo si inserisce, invece, in un percorso differente, seppur collegato, caratterizzato da un approccio più ampio e strutturale[6], in relazione a tutte le questioni relative alla intelligenza artificiale[7], partendo dalle finalità di impiego degli strumenti e dalle loro implicazioni etiche, sociali ed economiche. Questo percorso riflette la volontà dell'Unione europea di promuovere un modello di *governance* che bilanci l'innovazione tecnologica con la protezione dei diritti fondamentali, mediante l'introduzione di strumenti giuridici specifici, come il regolamento sull'intelligenza artificiale (*AI Act*)[8]. Tale divergenza nei percorsi normativi evidenzia i diversi livelli di complessità che coinvolgono gli strumenti considerati e la necessità di contestualizzare le norme in funzione delle specificità che caratterizzano ciascun ambito applicativo.

La strategia europea, quindi, si distingue per il suo tentativo di integrare considerazioni tecniche con questioni di ordine etico ed economico, mirando a stabilire un equilibrio tra l'incoraggiamento nei confronti dell'innovazione e la protezione dei diritti individuali. Tale approccio dimostra una consapevolezza delle implicazioni a lungo termine delle tecnologie emergenti e un desiderio di prevenire scenari in cui le stesse possano avanzare a scapito delle libertà fondamentali.

---

[6] Cfr. il capitolo I, § 3.

[7] Da qui in avanti IA.

[8] Cfr. *infra* il § 3.2.

2. *L'esperienza italiana e il SARI*

In Italia, la scelta di impiegare la tecnologia di riconoscimento facciale ha dato vita ad un acceso dibattito che, rispetto ai possibili rischi legati al suo utilizzo, non ha lasciato indifferente il Garante della privacy: l'Autorità ha svolto due istruttorie, tese a verificare la compatibilità dell'impiego di SARI con la disciplina posta a protezione dei dati personali [9].

Con riferimento alla modalità *enterprise*, al termine della fase di sperimentazione del software conclusa nel settembre 2018 [10], l'Autorità garante, con il provvedimento n. 440, ha osservato che «il trattamento (…) mediante il sistema SARI "*enterprise*", (…), non presenta criticità sotto il profilo della protezione dati» [11]. Secondo il Garante, l'impiego del sistema di riconoscimento facciale *a posteriori* [12] costituisce un mero ausilio tecnico finalizzato a supportare le attività di ricerca condotte all'interno dell'archivio AFIS [13]. In conformità all'art. 8 d.lgs. n. 51/2018 [14], il funzionamento dello strumento non risulta completamente automatizzato, prevedendo l'intervento di un operatore qualificato che si occupa dell'inserimento manuale nella maschera di interrogazione di specifici dati anagrafici, descrizioni somatiche e altre caratteristiche particolari. Seguendo il ragionamento del Garante, il sistema è stato progettato per accelerare il processo di identificazione da parte degli

[9] Per un rinvio al funzionamento di SARI cfr. il capitolo II, § 4.1. Per un approfondimento sul provvedimento cfr. R. LOPEZ, *Videosorveglianza biometrica tramite riconoscimento facciale: parere negativo del Garante per la privacy*, in *Proc. pen. e giust.*, 2022, p. 798 ss.; nonché E.C. RAFFIOTTA-M. BARONI, *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, in *BioLaw Journal-Riv. BioDir.*, 2022, p. 165 ss.

[10] Cfr. MINISTERO DELL'INTERNO, *Comunicato del 19.9.2018*, reperibile all'indirizzo https://www.interno.gov.it/it/notizie/sistema-automatico-riconoscimento-immagini-futuro-diventa-realta.

[11] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell'identità di un volto, n. 440/2018*, 26.7.2018, reperibile all'indirizzo https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9040256.

[12] Cfr. il capitolo II, § 4.

[13] Cfr. il capitolo II, § 4.2.

[14] Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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.

operatori di polizia, il cui intervento rimane imprescindibile per verificare l'attendibilità e l'accuratezza dei risultati generati dal sistema. Il software dunque si limiterebbe a svolgere un ruolo di ottimizzazione procedurale, lasciando tuttavia all'operatore umano il compito di impostare i parametri di ricerca e interpretare gli esiti ottenuti. Ne consegue che l'impiego della modalità *enterprise* del software «costituisce non un nuovo trattamento di dati personali, (…), bensì una nuova modalità di trattamento di dati biometrici, che dovrà essere effettuata nel rispetto delle regole previste dalla normativa rilevante in materia di tutela dei dati personali» [15]. Pertanto, il sistema non altera il perimetro dei dati accessibili, ma si limita unicamente a innovare le modalità operative di analisi e confronto.

Nel provvedimento si specifica che, in osservanza dell'art. 7 d.lgs. n. 51/2018, il ricorso a questo strumento risulta già previsto e disciplinato da diverse fonti normative e, nello specifico, quelle individuate nel d.m. 24 maggio 2017 [16]. Tra queste figurano: gli artt. 4 del TULPS e 7 del relativo regolamento di esecuzione relativi ai rilievi segnaletici – descrittivi, fotografici, dattiloscopici e antropometrici – che l'autorità di pubblica sicurezza può disporre nei confronti di soggetti considerati pericolosi o sospetti, o di coloro che non siano in grado o si rifiutino di provare la propria identità; l'art. 349 c.p.p. avente ad oggetto l'identificazione della persona indagata, che la polizia giudiziaria può effettuare attraverso rilievi dattiloscopici, fotografici, antropometrici e ulteriori accertamenti ove necessario; l'art. 5, comma 2-*bis*, d.lgs. 25 luglio 1998, n. 286 sui rilievi fotodattiloscopici previsti per gli stranieri richiedenti il permesso di soggiorno; nonché le disposizioni contenute nel provvedimento generale del Garante per la protezione dei dati personali in materia di biometria (n. 513 del 12 novembre 2014). Pertanto, nella sua funzione *enterprise*, SARI non farebbe altro che automatizzare un'attività che la polizia ha sempre svolto manualmente, in conformità ad una base normativa, sì frammentata ma sufficientemente chiara e precisa [17]. Secondo il

---

[15] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell'identità di un volto, n. 440/2018*, cit.

[16] Già richiamato al capitolo II, § 4.2. *Individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, attuazione dell'articolo 53, comma 3, del decreto legislativo 30 giugno 2003, n. 196 (17A04275).*

[17] Cfr. G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale*

Garante, dunque, il requisito della necessaria base giuridica per il trattamento dei dati può in questo caso ritenersi soddisfatto.

Anche il criterio della stretta necessità del ricorso allo strumento troverebbe giustificazione nel contesto pratico in cui tali sistemi operano. Senza l'ausilio dell'algoritmo, l'attribuzione dell'identità ad un sospettato, a partire da una semplice immagine, potrebbe rivelarsi un'operazione assai dispendiosa in termini di tempo, rischiando di risultare incompatibile con i termini imposti nella fase delle indagini preliminari. In questo senso, l'impiego del sistema automatizzato appare funzionale a garantire l'efficienza delle attività investigative, pur richiedendo un monitoraggio costante per assicurare il rispetto delle garanzie fondamentali.

Nonostante la visione ottimista e tendenzialmente rassicurante del Garante, persistono rilevanti criticità sul piano sistematico e applicativo, legate alla formulazione eccessivamente generica delle disposizioni normative di riferimento. In particolare, la mancanza di una delimitazione chiara e specifica dei contesti nei quali tali strumenti possono legittimamente essere impiegati solleva non trascurabili preoccupazioni sia sotto il profilo della legalità dell'azione amministrativa e giudiziaria, sia in relazione alla tutela dei diritti fondamentali degli individui coinvolti. Secondo alcuni Autori, la delega a margini ampi e indeterminati di discrezionalità in capo alle autorità giudiziarie si configura quale fattore di rischio potenzialmente incompatibile con i principi di legalità, proporzionalità e necessità che sovraintendono all'adozione di misure lesive della sfera privata e personale [18]. L'indeterminatezza delle condizioni giustificative del ricorso a questi strumenti potrebbe infatti tradursi in una contrazione eccessiva delle garanzie processuali minime previste tanto dall'ordinamento interno, quanto dal diritto sovranazionale [19].

A distanza di poco meno di tre anni, il Garante privacy ha avuto modo di esprimersi anche sulla modalità applicativa di SARI *real-time* [20]. In primo luogo, il sistema realizzerebbe un trattamento automatizzato su larga scala che potrebbe riguardare anche «persone presenti a manifestazioni politiche

---

automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario, in *Leg. pen.*, 11 dicembre 2021, p. 5.

[18] T. ALESCI, voce *Corpo dell'imputato (fonte di prova nel processo penale)*, in *Dig. disc. pen.*, Torino, 2018, p. 81.

[19] Cfr. il capitolo III.

[20] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time – 25 marzo 2021*, n. 127.

e sociali, che non sono oggetto di "attenzione" da parte delle forze di polizia»[21]. Infatti, «l'identificazione di una persona in un luogo pubblico comporta il trattamento biometrico di tutte le persone che circolano nello spazio pubblico monitorato, al fine di generare i modelli di tutti per confrontarli con quelli della *watch-list*»; pertanto, conclude l'Autorità, «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».

Il Garante ha ritenuto la modalità non conforme alla normativa europea che richiede una base giuridica adeguata, dal momento che «così come progettato, [porterebbe ad] una possibile forma di sorveglianza e identificazione di massa». Tra le varie disposizioni citate nella valutazione d'impatto, secondo il provvedimento, l'art. 1 TULPS disciplina in generale le funzioni dell'Autorità di pubblica sicurezza, senza operare alcun riferimento al trattamento di dati biometrici. Parimenti, alla luce delle considerazioni espresse dal Garante, gli artt. 134 comma 4, 234, 266 e 431 comma 1, lett. b), c.p.p. – aventi ad oggetto la documentazione degli atti con riproduzione audiovisiva, l'acquisizione di documenti mediante fotografia ed altri mezzi e l'intercettazione di flussi di comunicazioni telematiche o tra presenti mediante dispositivi elettronici portatili – non possono considerarsi una base giuridica idonea al trattamento dei dati biometrici finalizzato all'identificazione dell'individuo in modalità "*live*", dal momento che non prevedono l'acquisizione, l'estrazione e la comparazione di un volume di dati biometrico equivalente a quello richiesto dai sistemi di riconoscimento facciale *in tempo reale*. Ancora, gli artt. 55, 348, 354 e 370 c.p.p., concernenti le funzioni di polizia giudiziaria e aventi ad oggetto la tutela delle fonti di prova su luoghi o persone, di iniziativa o su delega dell'Autorità giudiziaria, non fanno alcuna menzione dei criteri da adottare in presenza di dati biometrici. Infine, il d.P.R. 15 gennaio 2018, n. 15, recante la disciplina del trattamento dei dati effettuato per le finalità di polizia include l'acquisizione di informazioni attraverso i sistemi di videosorveglianza e di ripresa fotografica, audio e video, «sistemi ontologicamente diversi da quelli che trattano dati biometrici»[22]. La distinzione si fonda sul fatto che i sistemi di videosorveglianza si limitano alla registrazione passiva delle immagini e dei suoni, senza necessariamente ricorrere a processi di estrazione automatizzata di caratteristiche biometriche.

---

[21] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time – 25 marzo 2021*, n. 127, cit.

[22] Il parere del Garante rimanda al considerando 51 del regolamento (UE) 2016/679.

Le suddette disposizioni non risultano dunque idonee per il soddisfacimento dei requisiti di specificità richiesti per il trattamento dei dati biometrici per finalità di sicurezza pubblica e repressione dei reati. La modalità applicativa *real-time* di SARI, secondo il Garante, consentirebbe di trattare, senza alcuna puntuale e specifica normativa di riferimento – e, dunque, illecitamente – le rappresentazioni digitali dei volti di una moltitudine di consociati al fine di confrontarli con quelle dei soggetti inseriti nella *watch-list.* Al contrario di quanto avviene con il sistema *enterprise*, infatti, in questo caso non siamo di fronte semplicemente ad una nuova modalità di gestione dei dati, già prevista e disciplinata da leggi o regolamenti, ma abbiamo a che fare con un nuovo e diverso trattamento non previsto da alcuna normativa in vigore.

2.1. *Il decreto "capienze" e l'inerzia del legislatore*

In risposta alla questione sollevata dal Garante nazionale, il legislatore italiano, nel tentativo di uniformarsi alla disciplina europea che, nel frattempo, era in via di definizione, ha predisposto un quadro normativo dominato dall'incertezza.

Inizialmente, la preoccupazione per un uso discriminatorio di questi sistemi e i rischi per la privacy a essi connessi, aveva spinto alcuni parlamentari a presentare un disegno di legge volto a sospendere l'impiego delle tecnologie in questione [23]. Nel preambolo del testo, infatti, si specificava che, considerato come risultino «ormai molti i comuni italiani, compresi i grandi capoluoghi che progettano di trasformare i loro sistemi di videosorveglianza in veri e propri sistemi di riconoscimento facciale», pur «in assenza di un quadro normativo che consenta di uniformare le condizioni per l'utilizzo dei dati biometrici», fosse necessaria una «moratoria per l'utilizzo dei sistemi di riconoscimento facciale nei luoghi pubblici o aperti al pubblico […]», fino a quando non sarebbe stata adottata una normativa nel pieno rispetto dei diritti costituzionali dei cittadini, conformemente alle indicazioni delle autorità nazionali ed europee per la protezione dei dati personali.

Tale iniziativa si è effettivamente tradotta in legge, con il d.l. n. 139/2021

[23] Cfr. il d.d.l. AC 3009, "*Sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici in luoghi pubblici o aperti al pubblico*", 12 aprile 2021.

(cd. decreto "capienze"), conv. in legge n. 205/2021 [24]. In particolare, l'art. 1, comma 9 dispone che «l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici di cui all'art. 4, n. 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» (termine poi prorogato al 2025) [25]. Tale moratoria però non si applica «ai trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali di cui al decreto legislativo 18 maggio 2018, n. 51, 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 reso ai sensi dell'articolo 24, comma 1, lettera b), del medesimo decreto legislativo n. 51 del 2018» [26]. La novella, da un lato, inibisce l'utilizzo del riconoscimento facciale automatizzato finché non venga introdotta una normativa puntuale per disciplinarlo, dall'altro, esclude dalla moratoria alcune finalità d'impiego, in particolare l'adozione da parte dell'autorità giudiziaria.

Un primo aspetto che merita attenzione concerne l'interpretazione della nozione di "autorità competente a fini di prevenzione e repressione dei reati" [27], nella quale risultano incluse anche le pubbliche amministrazioni. Tale estensione implica che i Comuni – e più in generale qualsiasi ente pubblico autorizzato all'esercizio di funzioni finalizzate alla prevenzione e alla sicurezza pubblica – possano legittimamente ricorrere a sistemi di videosorveglianza

---

[24] Cfr. il d.l. n. 139/2021 convertito con modificazioni in legge n. 205/2021 "*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*".

[25] Cfr. l'art. 9, comma 11, d.l. n. 139/2021. Il termine è stato poi prorogato dal 31 dicembre 2023 al 31 dicembre 2025 dalla legge n. 87/2023.

[26] Cfr. l'art. 9, comma 12, d.l. n. 139/2021.

[27] Cfr. la definizione di "autorità competente" contenuta nell'art. 3, par. 7 della direttiva 680/2016/UE che include «*a*) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; o *b*) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica».

integrati con software di riconoscimento facciale, anche in assenza di una normativa organica e specifica che disciplini i casi e le modalità di ricorso a tali strumenti. In questa prospettiva, emerge il rischio, in parte già concretizzato a livello nazionale [28], di una proliferazione disomogenea di iniziative locali, con conseguenti potenziali violazioni delle garanzie costituzionali e sovranazionali poste a presidio delle libertà individuali.

La medesima norma, caratterizzata da una formulazione che ha sollevato plurimi dubbi sul piano interpretativo [29], prevede poi l'obbligo di acquisire un parere favorevole da parte del Garante basato sulla valutazione d'impatto di questi sistemi. Tuttavia, appare del tutto improbabile che la stessa Autorità possa esprimere un giudizio favorevole rispetto all'implementazione di questi strumenti, soprattutto se si considera l'orientamento restrittivo adottato pochissimi mesi prima, come evidenziato nel provvedimento di diniego relativo all'impiego del sistema SARI *real-time* [30].

Ma allora, quale può essere stata l'effettiva *intentio legis*, se l'assenza di uno specifico quadro normativo di riferimento era proprio la ragione per la quale si era proposta inizialmente una sospensione dell'impiego di tali *tools?* Dalla stessa moratoria si esclude poi l'uso dei software di riconoscimento facciale da parte «dell'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali e di quelle del pubblico ministero» [31]. Tale deroga, che sottrae al divieto temporaneo di utilizzo una categoria specifica di soggetti istituzionali, sarebbe basata sulla necessità di preservare l'efficienza e la prontezza dell'azione giudiziaria, garantendo la piena operatività degli strumenti tecnologici avanzati, qualora impiegati nell'ambito di procedure sottoposte al controllo giurisdizionale o vincolate al rispetto delle garanzie processuali. Tuttavia, l'esclusione in esame solleva alcune rilevanti questioni sul piano sistematico, in particolare con riferimento al bilanciamento tra poteri pubblici e interessi individuali. Si tratta, infatti, di una scelta normativa che incide sulla natura e sulla qualità delle garanzie previste per i destinatari del trattamento, in quanto, pur riconoscendo la particolare rilevanza delle funzioni giurisdizionali e requirenti, finisce per legittimare l'adozione di

---

[28] Cfr. il capitolo I, § 2.

[29] Cfr. tra gli altri, J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale*, in I. MICHELI (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*, EUT Edizioni Università di Trieste, Trieste, 2023, p. 175.

[30] Cfr. il § precedente.

[31] Cfr. l'art. 9, comma 12, d.l. n. 139/2021.

tecnologie invasive senza una cornice di limiti altrettanto stringenti, quali quelli imposti ad altri soggetti pubblici o privati.

Inoltre, già ad una prima lettura della disposizione risulta immediatamente evidente la problematica di legittimità di un sistema che attribuisca alternativamente al giudice o al pubblico ministero la facoltà di determinare l'opportunità di ricorrere a strumenti di sorveglianza di tale natura, in assenza, nel secondo caso, di un meccanismo di convalida successiva [32]. In questa prospettiva, parrebbe preferibile attribuire in via esclusiva al giudice la competenza ad autorizzare l'impiego di tali strumenti, assicurando un controllo effettivo sull'adozione di misure potenzialmente invasive della sfera individuale.

Il testo, poi, non distinguendo fra modalità *in tempo reale* e *a posteriori*, sembra riferirsi ad un ricorso generalizzato del software a fini giudiziari e investigativi, che genera non poca confusione, oltreché inevitabili dubbi di legittimità costituzionale [33]. Le norme introdotte appaiono non conformi ai requisiti posti dagli articoli 13 Cost., 8 Conv. eur. dir. uomo, 7, 8 e 52 CDFUE, nonché dall'art. 10 LED [34]. Esse risultano infatti del tutto carenti nella definizione dei criteri e delle modalità attraverso cui le autorità competenti, quali le forze di polizia o la magistratura, possano avvalersi dei sistemi di riconoscimento facciale. Non emergono prescrizioni chiare e dettagliate in merito alle specifiche condizioni di utilizzo, alle finalità perseguibili o ai limiti procedurali, elementi essenziali per garantire la conformità dell'uso di tali strumenti ai principi di legalità e certezza del diritto. Ciò contrasta con i requisiti del quadro normativo europeo e le interpretazioni fornite sia dalla CGUE sia dalla Corte EDU [35].

La norma contenuta nel decreto, d'altra parte, nonostante l'estrema intrusività dello strumento, non stabilisce neppure che possa essere fatto ricorso alla tecnologia solo per reati di una certa gravità e unicamente laddove ciò sia strettamente necessario. La mancanza di questi elementi compromette la certezza del diritto, poiché non consente agli utenti e alle autorità di conoscere con precisione i confini dell'applicabilità di tali strumenti

---

[32] Sul punto cfr. F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Wolters Kluwer Cedam, Milano, 2020, p. 134.

[33] Cfr. il capitolo III, § 2 ss.

[34] Cfr. il capitolo III, § 4.

[35] Cfr. il capitolo III, § 4.

tecnologici. Ciò espone al rischio di abusi e discrezionalità e non garantisce un bilanciamento adeguato tra esigenze di sicurezza pubblica e tutela dei diritti fondamentali.

La disposizione manca infine l'occasione di specificare i termini di conservazione dei dati raccolti tramite la tecnologia di riconoscimento facciale. Va ricordato che il d.P.R. n. 15/2018, che disciplina il trattamento dei dati personali da parte delle forze di polizia [36], ha previsto – molto genericamente – che il trattamento dei dati biometrici sia consentito «quando è necessario per le esigenze di un'attività informativa, di sicurezza o di indagine di polizia giudiziaria o di tutela dell'ordine e della sicurezza ad integrazione di altri dati personali» [37]. Ai fini che qui rilevano, l'art. 10 comma 3, lett. u) del d.P.R. fa solo generico riferimento ai «dati raccolti mediante sistemi di ripresa fotografica, audio e video» e ai «dati raccolti mediante sistemi di videosorveglianza o di ripresa fotografica, audio e video di documentazione dell'attività operativa». La disposizione, infatti, pur fornendo indicazioni utili per delimitare i termini di conservazione dei *dati ricavati*, non offre una disciplina adeguatamente dettagliata per le ulteriori categorie, ossia quelli *trasformati/convertiti* e quelli *generati automaticamente.*

L'assenza di indicazioni specifiche, a fronte di limiti temporali di conservazione anche molto dilatati e riferiti a classi di informazioni generali, alla luce della normativa europea sulla protezione dei dati, potrebbe sollevare problematiche di compatibilità tra la disciplina interna e quella contenuta nell'art. 8 Conv. eur. dir. uomo, così come interpretata dalla Corte di Strasburgo [38]. Come visto, queste lacune rischiano di compromettere il delicato bilanciamento tra la necessità di garantire la sicurezza pubblica e la tutela dei diritti fondamentali, con particolare riferimento al diritto alla privacy e alla protezione dei dati personali.

Secondo una lettura condivisa, al fine di evitare un potenziale contrasto con i principi fondamentali dell'ordinamento, occorre adottare un'interpretazione costituzionalmente orientata della norma [39]. La controversa disposizione potrebbe dunque essere intesa non come volta a liberalizzare l'uso del riconoscimento facciale *in tempo reale*, bensì come norma "di conferma", finalizzata a ribadire che, nonostante la moratoria generale imposta sull'impiego di

[36] Attuativo della direttiva UE/2016/680.

[37] Cfr. l'art. 11, comma 2, d.P.R. n. 15/2018.

[38] Cfr. il capitolo III, § 4 ss.

[39] Cfr. J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale*, in I. MICHELI (a cura di), *Ragioni Comuni 2019-2020*, cit., p. 178.

queste tecnologie, le autorità di *law enforcement* possono continuare a utilizzarle solo nei limiti previsti dalle fonti normative sovraordinate e dal codice di procedura penale. Questa interpretazione sarebbe corroborata sul piano logico-sistematico: infatti, una lettura letterale della disposizione finirebbe per frustrare la *ratio legis*, stravolgendo l'obiettivo perseguito dal Parlamento che consisteva nell'introdurre limiti più stringenti per garantire un maggiore equilibrio tra le esigenze di sicurezza e la tutela dei diritti fondamentali. Pertanto, l'art. 9, comma 12, d.l. n. 139/2021, conv. in legge n. 205/2021, non può essere inteso come idoneo a legittimare indiscriminatamente l'utilizzo del riconoscimento facciale automatico, tanto più considerando la delicatezza del settore in cui l'adozione di strumenti tecnologici invasivi deve necessariamente conformarsi ai principi di proporzionalità, necessità e legalità.

3. *Il quadro normativo sovranazionale: verso un sistema armonizzato di regole*

Se a livello nazionale non è ancora stato introdotto uno strumento normativo che regoli organicamente le funzioni e le applicazioni dei sistemi di riconoscimento facciale, nell'Unione europea e, nel più ampio ambito del Consiglio d'Europa, da almeno due lustri, le istituzioni si stanno adoperando per delineare le "coordinate" normative e para-normative, in grado di orientare e disciplinare il comportamento degli operatori nel più ampio settore dell'intelligenza artificiale.

La corsa alla regolamentazione ha avuto origine circa nel 2017, quando si è aperto il dibattito sull'intelligenza artificiale con la *Risoluzione del Parlamento europeo sulla robotica*[40], che annunciava la nascita di robot intelligenti autonomi ed evocava la necessità di attribuire diritti e doveri a queste nuove entità[41]. Nello stesso atto compariva un invito espresso, formulato nei

[40] PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica* (2015/2103(INL)), v. https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A52017IP0051.

[41] Qualche settimana prima si colloca cronologicamente la Dichiarazione di Asilomar, alla cui redazione hanno partecipato ricercatori in materia di IA e robotica, nonché esperti di

confronti della Commissione europea, a considerare concretamente l'idea della creazione di un'agenzia per l'IA e a definire un quadro politico globale, al fine di mitigare i rischi di potenziali violazioni di diritti fondamentali.

Nel marzo del 2018, questa volta nel più esteso ambito del Consiglio d'Europa, è stato pubblicato l'interessante studio dal titolo "*Algorithms and Human Rights*" [42], nella cui sezione dedicata al *fair trial* si anticipavano alcune delle preoccupazioni affrontate poi a distanza di qualche mese dalla "*Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia*".

Appena un mese dopo, con la comunicazione "*L'intelligenza artificiale per l'Europa*" [43], la Commissione europea esordiva affermando che «l'intelligenza artificiale (IA) non è fantascienza: fa già parte delle nostre vite». In questa occasione, il messaggio fondamentale che la Commissione ha inteso diffondere è che sussiste «la necessità di unire le forze a livello europeo, per assicurare che tutti i cittadini europei partecipino alla trasformazione digitale, che risorse adeguate siano dedicate all'IA e che i valori e i diritti fondamentali dell'Unione siano in primo piano nel contesto dell'IA». L'impegno di fondo si snoda in due obiettivi distinti fondamentali: portare gli investimenti economici in questo ambito ad un livello più alto e garantire che le nuove tecnologie riflettano i "valori" fondamentali europei. Riguardo a questi, con la citata comunicazione, la Commissione europea ha preannunciato l'elaborazione di una serie di linee guida etiche per la regolamentazione dell'IA da parte di un gruppo indipendente di esperti ad alto livello, istituito dalla Commissione europea nel giugno 2018 [44]. Di lì, per la prima volta, è stato introdotto il concetto di "intelligenza artificiale affidabile" e "umanocentrica", conforme alla normativa e ai diritti fondamentali, oltre che "robusta" in termini di sicurezza, protezione e affidabilità.

---

tecnologia e studiosi di diritto, provenienti da università e organizzazioni internazionali. La dichiarazione si compone di ventitré raccomandazioni. Tra i principi richiamati nel documento si ricorda quello di trasparenza per i sistemi algoritmici impiegati nell'assunzione di una decisione giudiziaria e quello di conformità dei sistemi di IA ai diritti fondamentali. Il documento è consultabile sul sito dell'istituto Future of Life, *futureoflife.org.*

[42] Reperibile su https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5.

[43] Comunicazione COM(2018) 237 final – "*L'intelligenza artificiale per l'Europa*". Il testo è reperibile su https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52018DC0237.

[44] HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, *Ethics guidelines for trustworthy AI*, reperibili su https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Nella stessa occasione viene ribadito l'impegno dell'Unione europea a non produrre nuove forme di disuguaglianze, specialmente riferite a certe categorie di popolazione, ossia a «lavoratori, donne, persone con disabilità, minoranze etniche, bambini, consumatori o altri a rischio di esclusione». In quest'ottica, le linee guida hanno identificato quattro principi chiave, definiti "*imperatives*", per un'IA affidabile: il rispetto dell'autonomia umana, la prevenzione del danno, l'equità e l'esplicabilità, intesa come trasparenza e tracciabilità delle informazioni e del procedimento [45].

L'8 aprile 2019, con la pubblicazione delle *Ethics guidelines for trustworthy AI*, l'Unione europea ha introdotto un tassello ulteriore, ossia la concezione secondo cui la necessità di un'IA affidabile non debba essere considerata un obiettivo da raggiungere, ma il fondamento stesso di un sistema normativo completamente nuovo, le cui applicazioni potenzialmente più lesive dei diritti fondamentali devono essere sempre soggette a una previa valutazione d'impatto obbligatoria. Queste includono la sorveglianza di massa e l'uso delle cd. "armi autonome" [46]. Con specifico riferimento al primo fenomeno, le *Guidelines* raccomandano alle autorità degli Stati membri di emanare atti che garantiscano l'individuo da attività di identificazione e tracciamento, attraverso sistemi di riconoscimento biometrico basati sull'IA come i «*face recognition and other involuntary methods of identification using biometric data (i.e. lie detection, personality assessment through micro expressions, and automatic voice detection)*» [47]. L'utilizzo di tali strumenti dovrebbe essere consentito solo in circostanze eccezionali, come per esempio in caso di minacce per la sicurezza nazionale, ma comunque anche in tali occasioni l'impiego andrebbe autorizzato solo se basato sul rispetto dei diritti fondamentali [48]. Inoltre, le linee guida

[45] Cfr. *Ethics guidelines for trustworthy AI*, cit., p. 10.

[46] Cfr. *Ethics guidelines for trustworthy AI*, cit., p. 34.

[47] Cfr. *Ethics guidelines for trustworthy AI*, cit., p. 33.

[48] «*AI enables the ever more efficient identification of individual persons by both public and private entities. Noteworthy examples of a scalable AI identification technology are face recognition and other involuntary methods of identification using biometric data (i.e. lie detection, personality assessment through micro expressions, and automatic voice detection). Identification of individuals is sometimes the desirable outcome, aligned with ethical principles (for example in detecting fraud, money laundering, or terrorist financing). However, automatic identification raises strong concerns of both a legal and ethical nature, as it may have an unexpected impact on many psychological and sociocultural levels. A proportionate use of control techniques in AI is needed to uphold the autonomy of European citizens. Clearly defining if, when and how AI can be used for automated identification of individuals and differentiating between the*

hanno posto in luce la necessità di introdurre una chiara definizione dei casi in cui può essere impiegata l'IA finalizzata al riconoscimento automatizzato degli individui e la precisa distinzione fra «*identification of an individual, versus the tracing and tracking of an individual, and between targeted surveillance and mass surveillance*»[49]. Tale indirizzo è lo stesso che sembra muovere il Consiglio dell'Unione europea che, nelle Conclusioni sul piano coordinato per lo sviluppo e l'uso dell'IA[50], ha posto in luce la necessità di garantire un utilizzo dei nuovi sistemi di IA nel rispetto dei valori dell'Unione europea e dei diritti fondamentali dell'uomo.

Quasi contestualmente, nell'ambito del Consiglio d'Europa, si colloca l'adozione da parte della Commissione europea per l'efficienza della giustizia (CEPEJ) della già citata *Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia* e dei principi in essa enunciati[51], nel cui Preambolo i legislatori nazionali sono stati invitati a «stabilire una cornice normativa entro la quale i nuovi strumenti vadano sviluppati, verificati e utilizzati» e a fruire di un elenco di valori ineludibili per aderire a una forma di intelligenza artificiale che aspiri a porsi come «antropocentrica e affidabile». Il documento è rivolto principalmente agli «attori pubblici e privati incaricati di creare e lanciare strumenti e servizi di intelligenza artificiale relativi al trattamento di decisioni e dati giudiziari», nonché ai «responsabili di decisioni pubbliche competenti, o dello sviluppo, della verifica o dell'utilizzo di tali strumenti e servizi»[52].

---

identification of an individual vs the tracing and tracking of an individual, and between targeted surveillance and mass surveillance, will be crucial for the achievement of Trustworthy AI. The application of such technologies must be clearly warranted in existing law. Where the legal basis for such activity is "consent", practical means must be developed which allow meaningful and verified consent to be given to being automatically identified by AI or equivalent technologies. This also applies to the usage of "anonymous" personal data that can be re-personalised». Cfr. *Ethics guidelines for trustworthy AI*, cit., p. 33-34.

[49] Cfr. HIGH-LEVEL EXPERT GROUP ON AI, *Ethics guidelines for trustworthy AI,* 2019, p. 33, reperibili su https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

[50] Le conclusioni del Consiglio dell'Unione europea sono reperibili su https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/it/pdf.

[51] Cfr. CEPEJ – *European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment*, reperibile su https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment.

[52] Cfr. CEPEJ – *European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment*, cit., p. 5.

Trattasi di un significativo documento di *soft law* che muove dalla consapevolezza che l'IA sia in grado di generare enormi vantaggi per gli individui e per la società, ma porti con sé anche determinati rischi che vanno gestiti in modo adeguato. In tale ottica si afferma la necessità di assicurare «l'efficienza e la qualità della giustizia […], nel dovuto rispetto dei diritti fondamentali della persona, enunciati nella Convenzione europea sui diritti dell'uomo e nella Convenzione per la protezione dei dati di carattere personale, e in conformità agli altri principi fondamentali esposti in prosieguo, che dovrebbero orientare la definizione delle politiche pubbliche in materia di giustizia in questo campo»[53]. Ne deriva un approccio completamente antropocentrico all'IA che postula il rispetto della dignità e dell'autonomia delle persone, alle quali va sempre garantito un potere di supervisione sulle macchine[54].

Più nel dettaglio, i principali obiettivi sono il rispetto dei diritti fondamentali nella progettazione e nell'applicazione di sistemi di IA; il divieto di discriminazione legata al rischio di immissione di *input* non neutri; una garanzia di qualità e di sicurezza dei dati e delle decisioni giudiziarie da utilizzare per l'elaborazione mediante sistemi computazionali, solo se integri, intangibili e provenienti da fonti affidabili; una garanzia di trasparenza, imparzialità e *fairness* in modo da assicurare, tramite i requisiti di accessibilità, comprensibilità e verificabilità esterna dei processi computazionali relativi all'analisi dei dati giudiziari; infine, la facoltà di controllo da parte dell'utente. Un *focus* particolare è stato poi posto sul divieto di decisioni basate unicamente su un trattamento automatizzato che ha suggerito in dottrina «gli spunti per un'urgente discussione tra scienze penali e informatiche»[55].

Nonostante la sua natura di documento di *soft law*, la Carta Etica ha prodotto un impatto significativo su numerose iniziative successive. I principi enunciati dalla CEPEJ e, più in generale, l'appello formulato nel documento a considerare i diritti fondamentali come quadro di riferimento essenziale per lo sviluppo della regolamentazione nel settore dell'IA, sono stati ampiamente recepiti e richiamati in numerosi documenti normativi e politici. Tale

---

[53] Cfr. CEPEJ – *European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment*, cit., p. 5.

[54] Su questo punto v. M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, cit., p. 15.

[55] Cfr. S. QUATTROCOLO, *Intelligenza artificiale e giustizia nella cornice della Carta etica europea. Gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *Leg. pen.*, 18 dicembre 2018.

diffusione evidenzia il ruolo cruciale della Carta come strumento di orientamento per la costruzione di un modello regolativo che coniughi innovazione tecnologica e salvaguardia dei principi fondamentali [56].

3.1. *Dal Libro bianco della Commissione europea alla Convenzione sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto nell'ambito del Consiglio d'Europa*

In una prospettiva più programmatica, prosegue l'azione dell'Unione europea con il *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia* del 19 febbraio 2020, tramite il quale, adottando un approccio normativo basato sul rischio di potenziale lesione dei diritti fondamentali, la Commissione europea ha espresso il duplice obiettivo di promuovere l'adozione dell'IA e di affrontare i rischi – quali meccanismi decisionali opachi, discriminazioni basate sul genere o di altro tipo, intrusioni nella vita privata degli individui o utilizzi per scopi criminali [57]. Tale approccio sembra offrire il concreto vantaggio di poter adattare la specifica norma alla rilevanza degli interessi giuridici coinvolti, al potenziale danno previsto e all'evitabilità delle potenziali violazioni da parte delle persone interessate. Comincia a profilarsi la possibilità di introdurre delle vere e proprie "classi di rischio" rispetto ai diversi usi dei sistemi di IA, che troveranno poi espressa previsione solo con il regolamento recentemente introdotto. Il *White Paper*, definendo le specifiche opzioni politiche su come ottenere lo scopo predetto, parte dal presupposto che il rapido sviluppo dell'intelligenza artificiale abbia determinato profondi cambiamenti nei modelli di produzione e di erogazione di servizi, migliorando l'assistenza sanitaria, aumentando l'efficienza dell'agricoltura, contribuendo alla mitigazione dei cambiamenti climatici e all'adattamento ai medesimi,

[56] La Carta etica ha ispirato altresì l'adozione dell'*AI Bill of Rights s*tatunitense, documento non vincolante che indica i principi cui dovrebbero essere orientati lo sviluppo e l'impiego dei sistemi algoritmici, affinché possa essere assicurata la protezione dei cittadini americani. Cfr. L. FLORIDI-E. HINE, *The Blueprint for an AI Bill of Rights: In Search of Enaction, at Risk of Inaction*, in *Minds and Machines*, 33, 2023, p. 285-292.

[57] Cfr. COMMISSIONE EUROPEA [COM (2020,) 65 final], *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, consultabile sul sito internet della Commissione. Esso è espressamente condiviso dalle *Conclusioni del Consiglio dell'Unione Europea*, "Accesso alla giustizia – Cogliere le opportunità della digitalizzazione", in *GUUE*, 14 ottobre 2020, C-342, 42 ss., p. I/6.

implementando l'efficienza dei sistemi di produzione e accrescendo generalmente la sicurezza dei cittadini europei.

In tal senso, la Commissione europea raccomanda agli Stati e alle istituzioni europee l'elaborazione di strategie comuni e unitarie per affrontare l'attuale trasformazione e le sfide del futuro con maggiore consapevolezza e responsabilità. Più specificamente, con questo documento la Commissione europea evidenzia le potenziali implicazioni per i diritti fondamentali derivanti dall'impiego a distanza di sistemi di riconoscimento biometrico e, più in particolare, della tecnologia di riconoscimento facciale [58]. L'impiego di quest'ultima può essere concesso soltanto quando debitamente motivato, proporzionato e soggetto a garanzie adeguate. Per prevenire eventuali violazioni di diritti fondamentali, poi, la Commissione europea ha proposto di identificare le specifiche circostanze di tempo e di spazio che potrebbero giustificare tale uso e alcune garanzie da adottare.

Sono seguite le *Conclusioni del Consiglio dell'Unione europea sulla Carta dei diritti fondamentali nel contesto dell'intelligenza artificiale e della trasformazione digitale*, nelle quali sono state poste in luce l'opacità, la complessità, la distorsione e un certo grado di imprevedibilità in alcuni comportamenti definiti "parzialmente autonomi" di determinati sistemi di IA, al fine di denunciare la loro attuale incompatibilità con i diritti fondamentali e facilitare l'introduzione di norme giuridiche [59].

Sulla scia tracciata dalle *Conclusioni* del Consiglio, il Parlamento ha adottato una serie di risoluzioni concernenti l'utilizzo dell'IA, riguardo, in particolare, all'etica [60], alla responsabilità [61] e in materia di *copyright* [62]. A queste sono seguite le risoluzioni sull'IA in materia penale [63] e nel settore

---

[58] Cfr. COMMISSIONE EUROPEA [COM (2020,) 65 final], *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, consultabile sul sito internet della Commissione, p. 24.

[59] Cfr. *Conclusioni della Presidenza – La Carta dei diritti fondamentali nel contesto dell'intelligenza artificiale e del cambiamento digitale*, 11481/20, 2020.

[60] Cfr. *Risoluzione del Parlamento europeo del 20 ottobre 2020 su un quadro degli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate*, 2020/2012(INL).

[61] Cfr. *Risoluzione del Parlamento europeo del 20 ottobre 2020 su un regime di responsabilità civile per l'intelligenza artificiale*, 2020/2014(INL).

[62] Cfr. *Risoluzione del Parlamento europeo del 20 ottobre 2020 sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale*, 2020/2015(INI).

[63] Cfr. *Relazione del Parlamento europeo sull'intelligenza artificiale nel diritto penale e suo utilizzo da parte della polizia e delle autorità giudiziarie in materia penale*, 2020/2016(INI).

dell'istruzione, della cultura e dell'audiovisivo [64]. Peraltro, in occasione della risoluzione sull'IA in materia penale, la Commissione per le libertà civili, la giustizia e gli affari interni ha chiesto espressamente una moratoria sulla diffusione dei sistemi di riconoscimento facciale a fini di contrasto e repressione dei reati nello spazio euro-unitario, affermando che «l'attuale stato di avanzamento di tali tecnologie e il loro impatto significativo sui diritti fondamentali richiedono un dibattito sociale aperto e approfondito, al fine di esaminare le diverse problematiche sollevate e la giustificazione di una loro diffusione» [65].

Il Parlamento europeo negli ultimi anni ha chiesto più volte di limitare, se non addirittura vietare in specifiche circostanze [66], l'impiego di siffatti strumenti. In più di un'occasione, è stato evidenziato che la raccolta a distanza e l'uso di dati biometrici per scopi di identificazione (in cui rientrerebbero certamente i sistemi di riconoscimento facciale) in spazi aperti al pubblico comporta rischi rilevanti per i diritti fondamentali [67]. In questa prospettiva, l'istituzione ha invitato la Commissione a considerare l'introduzione di una moratoria sull'impiego di questi strumenti negli spazi pubblici, nei luoghi di istruzione e della sanità, finché «*the technical standards can be considered fully fundamental rights-compliant, the results derived are non-biased and non-discriminatory, and there are strict safeguards against misuse that ensure the necessity and proportionality of using such technologies*» [68].

Nell'ambito del Consiglio d'Europa, l'11 settembre 2019, il Comitato

---

[64] Cfr. 2020/2017(INI).

[65] Cfr. *Relazione del Parlamento europeo sull'intelligenza artificiale nel diritto penale e suo utilizzo da parte della polizia e delle autorità giudiziarie in materia penale*, cit., p. 9.

[66] Cfr. *Risoluzione del Parlamento europeo del 19 maggio 2021 sull'intelligenza artificiale nell'istruzione, nella cultura e nel settore audiovisivo*, 2020/2017(INI).

[67] Cfr. *Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate*, 2020/2012(INL).

[68] Cfr. *Risoluzione del Parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale (2020/2013(INI)); 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))*. Per un approfondimento sulla risoluzione cfr. G. BARONE, *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della Risoluzione del Parlamento europeo del 6 ottobre 2021*, in *Cass. pen.*, 3, 2022, p. 1180.

dei Ministri ha deciso di istituire una Commissione *ad hoc* sull'IA (CAHAI) [69], cui è stato assegnato il compito di elaborare il primo trattato di diritto internazionale in tema di intelligenza artificiale, la c.d. *Convenzione quadro sull'Intelligenza Artificiale e i diritti umani, la democrazia e lo Stato di diritto*, adottata il 17 maggio 2024 [70]. Il documento è stato finalizzato in seno al CAI [71], comitato "successore" del CAHAI, incline ad abbracciare una prospettiva "*human rights based*" il cui scopo è stato quello di garantire che, nel contesto internazionale, le attività ricomprese nell'intero ciclo di vita dei sistemi di IA siano rispettose dei diritti fondamentali e della democrazia [72].

3.2. *Il regolamento europeo sull'intelligenza artificiale*

Tornando nell'ambito dell'Unione europea, nell'agosto 2024 è stato pubblicato nella Gazzetta Ufficiale UE il regolamento UE 2024/1689 in materia di IA, anche noto come *AI Act*, punto di arrivo delle precedenti iniziative di *soft law*, qui brevemente richiamate, e primo atto legislativo al mondo che disciplina il settore, promuovendo lo sviluppo e l'utilizzo di *tools* algoritmici sicuri ed affidabili all'interno del mercato unico europeo. Già nella proposta

---

[69] Cfr. https://www.coe.int/en/web/artificial-intelligence/cahai.

[70] Per un approfondimento cfr. A. HARS, *Conceptual Difficulties in the Transformation of Human Rights to the Realm of Artificial Intelligence*, in *Acta Humana*, 2, 2024, p. 123 ss.; F.P. LEVANTINO-F. PAOLUCCI, *Advancing The Protection Of Fundamental Rights Through AI Regulation: How The Eu And The Council Of Europe Are Shaping The Future*, in *SSRN*, 2024, p. 1-16.

[71] Il CAI è il comitato che è stato incaricato di istituire un processo di negoziazione internazionale per la predisposizione di un quadro giuridico sullo sviluppo, la progettazione e l'applicazione dell'IA nell'ambito del Consiglio d'Europa. Appena tre mesi prima, anche l'Assemblea generale delle Nazioni Unite ha adottato all'unanimità una risoluzione intitolata "*Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*". Con il documento, l'Assemblea riconosce che l'organizzazione delle Nazioni Unite, coerentemente con il suo mandato, contribuisce in modo unico a raggiungere un consenso globale su sistemi di intelligenza artificiale sicuri, protetti e affidabili, che sia coerente con il diritto internazionale, in particolare con la Carta delle Nazioni Unite e la Dichiarazione universale dei diritti umani. Cfr. https://digitallibrary.un.org/record/4040897?ln=en&v=pdf.

[72] Per un approfondimento cfr. C. NARDOCCI, *La (seconda) svolta del 2024. Anche il Consiglio d'Europa decide di regolamentare l'intelligenza artificiale*, in *BioLaw Journal-Riv. di BioDiritto,* Special Issue 1, 2024.

dell'aprile 2021[73], si evidenziavano i valori fondamentali a cui è ispirata l'azione dell'Unione europea in questo ambito, mirando a fornire agli utenti la fiducia necessaria per servirsi di strumenti basati sull'IA e incoraggiando al contempo le imprese a svilupparli[74].

Al fine di assicurare la massima uniformità a livello europeo e internazionale, è stata adottata un'ampia definizione di "sistema di intelligenza artificiale", inteso come «sistema automatizzato progettato per funzionare con livelli di autonomia variabili [...] che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali». La scelta è stata quella di adottare la stessa nozione della *Raccomandazione sull'Intelligenza Artificiale dell'OCSE*, astratta e flessibile, allo scopo di assicurare la c.d. neutralità tecnologica e, quindi, l'applicabilità del regolamento senza necessità di continue modifiche o integrazioni[75].

Rispetto all'iniziale proposta della Commissione UE, il regolamento si mostra più attento alla protezione dei diritti fondamentali, tra i quali vengono ribaditi «il diritto alla dignità umana, il rispetto della vita privata e della vita familiare, la protezione dei dati personali, la libertà di espressione e di informazione, la libertà di riunione e di associazione e il diritto alla non discriminazione, il diritto all'istruzione, la protezione dei consumatori, i diritti

---

[73] Cfr. la *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione, COM/2021/206 final;* cfr. anche il *Piano coordinato sull'intelligenza artificiale 2021*, reperibile su https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review.

[74] Cfr. G. DE GREGORIO, *The Digital Services Act: A Paradigmatic Example of European Digital Constitutionalism*, in *Diritti Comparati*, 17 maggio 2021, p. 1; M. EBERS-V.R.S. HOCH-F. ROSENKRANZ-H. RUSCHEMEIER-B. STEINRÖTTER, *The European Commission's Proposal for an Artificial Intelligence Act–A Critical Assessment by Members of the Robotics and AI Law Society*, in *(RAILS). J.* 4(4), 2021, p. 589-603; L. FLORIDI, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in *Philos. Technol.*, 34, 2021, p. 215-222; M. HILDEBRANDT, *The Proposal for an EU AI Act of 21 April 2021*, in *Brief Commentary*, 2021, reperibile su https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legalrequirements/F2662611_en.

[75] Cfr. *Explanatory Memorandum on the updated OECD definition of an AI system*, https://www.oecd-ilibrary.org/docserver/623da898en.pdf?expires=1722520019&id=id&accname=guest&checksum=71863626A100B8ADF8E04D28B7E EC7C. Cfr. S. RUSSEL-K. PERSET-M. GROBELNIK, *Updates to the OECD's definition of an AI system explained*, 29.11.2023, reperibile su https://oecd.ai/en/wonk/ai-system-definition-update.

dei lavoratori, i diritti delle persone con disabilità, l'uguaglianza di genere, i diritti di proprietà intellettuale, il diritto a un ricorso effettivo e a un giudice imparziale, i diritti della difesa e la presunzione di innocenza e il diritto a una buona amministrazione»[76]. Tra i valori richiamati, compaiono per la prima volta la «protezione dell'ambiente» e la prevenzione degli effetti causati dal «cambiamento climatico», rispetto ai quali nei prossimi mesi occorrerà che le autorità del mercato interno valutino la conformità dei primi risultati dei sistemi di IA[77].

La base giuridica del regolamento è stata (inaspettatamente) individuata nell'art. 114 TFUE che consente di adottare misure volte al riavvicinamento delle disposizioni nazionali relative all'instaurazione e al funzionamento del mercato interno[78]. Su questo ampio presupposto, la Commissione europea ha redatto un documento che si pone un obiettivo che va ben oltre l'area del mercato interno digitale, ossia quello di garantire che lo sviluppo tecnologico sia conforme ai diritti fondamentali degli individui e non solo dei semplici consumatori[79]. Nel dibattito scientifico scatenato dal testo normativo non sono mancati gli interrogativi e le perplessità sulle ragioni per le quali un regolamento volto alla protezione di diritti fondamentali, e riferito dunque alla dimensione costituzionale in senso ampio del sistema, incastoni le disposizioni entro il contesto delle esigenze di mercato. Questo aspetto ha catturato sin da subito l'attenzione degli interpreti, spostando il focus dalla sfera commerciale e del diritto privato ad un contesto molto più ampio, in cui l'intelligenza artificiale non è solamente una caratteristica di un prodotto o di un servizio, ma una dimensione complessa che richiede un delicato bilanciamento di interessi contrapposti. Il nesso tra la protezione di diritti fondamentali e la natura economica e commerciale dei prodotti di IA va senza dubbio individuato nell'esigenza di definire degli standard comuni che prevengano il più possibile il cattivo funzionamento del mercato interno; tale base

---

[76] Considerando 48.

[77] Considerando 130.

[78] Cfr. *ex multis* S. QUATTROCOLO, *Intelligenza artificiale e processo penale: le novità dell'Ai Act*, in *Dir. dif.*, 2025; A. ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa University Press, Pisa, 2020, p. 36.

[79] Cfr. S. QUATTROCOLO-E. SACCHETTO, *EU & AI: Lessons to be learned*, in E. LIM-P. MORGAN (eds.), *Private Law and Artificial Intelligence*, Cambridge University Press, Cambridge, 2024, p. 645.

giuridica consente, peraltro, l'adozione di un regolamento[80], permettendo l'introduzione di un quadro normativo uniforme[81], che copra l'intero processo di produzione, commercializzazione, vendita e utilizzo dell'intelligenza artificiale all'interno dell'Unione europea.

Come già osservato in altri atti e documenti, la Commissione richiama i numerosi benefici nell'ambito industriale e in generale nelle attività sociali derivanti dall'impiego di sistemi di IA. Migliorando e ottimizzando il libero scambio di prodotti e servizi, l'uso dell'IA è in grado di fornire vantaggi competitivi alle aziende e supportare così il raggiungimento di obiettivi in diversi settori[82]. Fa da contraltare la possibilità che la fruizione di talune applicazioni dei sistemi di intelligenza artificiale possa talora causare addirittura dei danni, sia materiali sia immateriali, ai singoli individui, «*per la salute, la sicurezza e i diritti fondamentali*». Per questa ragione, l'approccio che guida l'intero documento, costituto da 113 articoli e 13 allegati, è quello del "rischio" di violazione di diritti fondamentali degli individui, già presente, ma

[80] Giova ricordare che non sono mancate le critiche circa l'opportunità di ricorrere allo strumento del regolamento per disciplinare in modo organico l'impiego dell'intelligenza artificiale, ritenuto da alcuni un veicolo normativo inadeguato a regolare una materia che, per la sua natura sensibile e trasversale, avrebbe richiesto l'adozione di una direttiva maggiormente rispettosa delle specificità dei singoli ordinamenti giuridici nazionali. Tali osservazioni troverebbero un riscontro sistematico nella recente iniziativa del Consiglio d'Europa, che ha adottato un approccio complementare rispetto a quello di matrice eurounitaria (cfr. il § 3.1). La Convenzione si caratterizza per un'impostazione chiaramente orientata alla responsabilizzazione degli Stati contraenti e degli attori istituzionali pubblici, configurandosi come uno strumento volto a garantire l'implementazione progressiva ed effettiva di tutele normative legate ai diritti fondamentali, alla democrazia e allo Stato di diritto nel ciclo di vita dei sistemi di intelligenza artificiale. L'art. 1, comma 2, chiarisce con formulazione inequivoca che: «*Each Party shall adopt or maintain appropriate legislative, administrative or other measures to give effect to the provisions set out in this Convention. These measures shall be graduated and differentiated as may be necessary in view of the severity and probability of the occurrence of adverse impacts on human rights, democracy and the rule of law throughout the lifecycle of artificial intelligence systems. This may include specific or horizontal measures that apply irrespective of the type of technology used*». Cfr. S. QUATTROCOLO, *Intelligenza artificiale e processo penale: le novità dell'Ai Act*, in *Dir. dif.*, 2025.

[81] Cfr. S. QUATTROCOLO, *Intelligenza artificiale e processo penale: le novità dell'AI ACT*, cit., p. 2 e A. ADINOLFI, *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, in *I Post di AISDUE, V (2023), Sezione "Atti convegni AISDUE"*, n. 15, 14 marzo 2023, p. 337.

[82] Quali quelli sanitario, agricolo, educativo, della gestione delle infrastrutture, dell'energia, dei trasporti, della logistica, dei servizi pubblici, della sicurezza e della mitigazione e adattamento ai cambiamenti climatici.

diversamente declinato nel *White Paper*[83]. Mentre alcuni impieghi di sistemi di IA ritenuti "a rischio inaccettabile" sono stati vietati, altri, rientranti nella categoria "ad alto rischio", sono sottoposti a una serie di requisiti prescrittivi, tecnicamente anche molto dettagliati, che, a tratti, evocano l'impianto normativo del regolamento (UE) 2016/679[84]: dall'elaborazione di una puntuale e specifica valutazione d'impatto sui diritti fondamentali, alla garanzia di tracciabilità dei risultati, dalla costante supervisione umana nell'utilizzo di tali tecnologie, alla richiesta di assicurare un elevato livello di robustezza, sicurezza e accuratezza generale.

Parimenti con quanto previsto dalla normativa a protezione dei dati personali[85], in capo al produttore del sistema di intelligenza artificiale, il regolamento ha posto l'onere di svolgere un cd. "*conformity assessment*", prima che il prodotto sia messo in commercio, per dimostrare che i requisiti siano stati rispettati. A tal proposito, un ruolo di particolare rilevanza è svolto dagli standard tecnici elaborati al fine di garantire un'applicazione uniforme[86]. Con riferimento a questo, non sono mancate le preoccupazioni sul ruolo di particolare rilevanza attribuito agli organismi di standardizzazione: tali enti operano attraverso procedure decisionali che spesso mancano di trasparenza, rappresentatività e supervisione giurisdizionale, sollevando dubbi

---

[83] Per un approfondimento, cfr. G. DE GREGORIO-P. DUNN, *The European risk-based approaches: Connecting constitutional dots in the digital age*, in *Common Market Law Review*, 59(2), 2022, p. 473-500.

[84] Cfr. regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE. Cfr. il capitolo III, § 4. Per un approfondimento, N. MENÉNDEZ-G. MOBILIO, *Between prohibited risks and high risks: the regulation of facial recognition technology*, in O. POLLICINO-F. DONATI-G. FINOCCHIARO-F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, Giuffrè, Milano, 2025, p. 217.

[85] Il principale strumento di *assessment* è rappresentato dal registro delle attività di trattamento e dallo svolgimento di idonee valutazioni del rischio che il trattamento stesso può comportare nei confronti dell'interessato. Cfr. l'art. 35 GDPR.

[86] Cfr. EDRi, *The role of standards and standardisation processes in the EU's Artificial Intelligence (AI) Act*, 2022, in *www.edri.org.*, EUROPEAN COMMISSION, *Commission implementing decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence*, C(2023)3215, 2023. Per un approfondimento cfr. C. GALLESE, *La standardizzazione nell'AI Act*, in O. POLLICINO-F. DONATI-G. FINOCCHIARO-F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, Giuffrè, Milano, 2025, p. 305 ss.

sulla legittimità e sull'equità del processo di elaborazione degli standard [87]. Queste caratteristiche portano con sé il rischio che gli standard riflettano maggiormente gli interessi economici e tecnici delle grandi aziende del settore e conducano alla definizione di criteri tecnici che non garantiscono un adeguato livello di protezione dei diritti fondamentali, compromettendo l'efficacia del quadro normativo previsto dal regolamento.

Entro tale scenario, l'Ufficio IA che farà parte del *Directorate-General for Communication Networks, Content and Technology (o Directorate-General*), interno alla Commissione europea, si occuperà di facilitare l'applicazione pratica delle disposizioni. Lo scopo principale di questo nuovo ufficio sarà quello di fornire orientamenti e linee guida, verificando eventuali violazioni e richiedendo direttamente ai fornitori di intraprendere azioni correttive [88].

In questi mesi, gli Stati membri stanno iniziando ad adoperarsi per dare attuazione alle disposizioni programmatiche dell'AI Act e, più in generale, per adeguare la normativa interna a tutti quegli adempimenti che il regolamento richiede ai singoli Stati (cfr. § seg.). L'Italia è stata uno dei primi paesi europei ad attivarsi in questo senso ed il 20 maggio 2024 ha sottoposto all'*iter* di approvazione parlamentare il d.d.l. S-1146 rubricato "*Disposizioni e delega al Governo in materia di intelligenza artificiale*" [89], il cui obiettivo è quello «di operare un bilanciamento tra [le] opportunità e [i] rischi insiti nella moderna era dell'intelligenza artificiale, accompagnando il quadro regolatorio [europeo] in quegli spazi propri del diritto interno» [90].

---

[87] Cfr. M. EBERS, *Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act*, in L.A. DIMATTEO-M. CANNARSA-C. PONCIBÒ (eds.), *The Cambridge Hankdbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, Cambridge University Press, Cambridge, 2022, p. 321 ss. Più in generale sul tema cfr. H. SCHAPEL, *The New Approach to the New Approach: The Juridification of Harmonized Standards in EU Law*, in *Maastr. Journ. of Eur. and Comp. Law*, 20(4), 2013, p. 521-533.

[88] Cfr. https://digital-strategy.ec.europa.eu/it/node/12445.

[89] Le norme interverranno su cinque ambiti: la strategia nazionale, le autorità nazionali, le azioni di promozione, la tutela del diritto di autore e le sanzioni penali. Con specifico riferimento al settore giudiziario, si introduce a livello nazionale il principio per il quale l'utilizzo dell'IA venga consentito esclusivamente per finalità strumentali e di supporto, quindi per l'organizzazione e la semplificazione del lavoro giudiziario nonché per la ricerca giurisprudenziale e dottrinale anche finalizzata all'individuazione di orientamenti interpretativi. Inoltre, viene specificato che dev'essere sempre riservata al magistrato la decisione sull'interpretazione della legge, la valutazione dei fatti e delle prove e sull'adozione di ogni provvedimento inclusa la sentenza. Per un approfondimento cfr. G. BARONE, *La regolamentazione dell'Intelligenza Artificiale: è "corsa agli armamenti"*, in *Dir. pen. e proc.*, 8, 2024, p. 994.

[90] I settori strategici individuati sono stati l'ambito sanitario e delle disabilità (artt. 7, 8 e

A completamento del quadro normativo delineato a livello europeo, a dicembre 2024 è entrata in vigore la nuova direttiva in materia di responsabilità per i danni derivanti da prodotti difettosi (cd. "*Product Liability Directive*") [91], la cui applicazione si estenderà anche ai beni digitali, ivi inclusi quelli integrati con componenti basate sull'intelligenza artificiale. Le peculiarità degli strumenti di IA, tra cui i vari gradi di autonomia e la loro *opacità*, possono rendere difficile o eccessivamente costoso, per quanti subiscano un danno, individuare il soggetto responsabile e dimostrare che sussistano i presupposti ai fini dell'esito positivo di un'azione di responsabilità [92]. La novità più rilevante concerne il sostanziale alleggerimento dell'onere della prova per i soggetti danneggiati, imponendo agli operatori economici di divulgare

9); il lavoro (artt. 10, 11 e 12); la pubblica amministrazione (art. 13); l'attività giudiziaria (artt. 14 e 15); la cybersicurezza nazionale (art. 16). Per un approfondimento sul tema cfr. G. BARONE, *La regolamentazione dell'Intelligenza Artificiale: è "corsa agli armamenti"*, in *Dir. pen. e proc.*, 2024, 8, p. 994 ss.

[91] Cfr. la direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio del 23 ottobre 2024 sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio, PE/7/2024/REV/1.Per un approfondimento cfr. M.C. BUITEN-A. DE STREEL-M. PEITZ, *The law and economics of AI liability*, in *Comp. Law & Sec. Rev.*, 48, 2023, p. 18; J. DE BRUYNE-O. DHEU-C. DUCUING, *The European Commission's approach to extra-contractual liability and AI – An evaluation of the AI liability directive and the revised product liability directive*, in *Comp. Law & Sec. Rev.*, 51, 2023; S. WACHTER, *Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond*, in *YJLT*, 26(3), 2024, p. 671-716.

[92] *Risoluzione del Parlamento europeo del 3 maggio 2022 sull'intelligenza artificiale in un'era digitale* (2020/2266 (INI)). In tale prospettiva, nel 2022 era stata avanzata una proposta di direttiva specificamente dedicata all'adeguamento del diritto dell'Unione europea in materia di responsabilità civile extracontrattuale all'impiego di sistemi di intelligenza artificiale (COM(2022) 496 final). L'iniziativa normativa si inseriva nel più ampio processo di costruzione di un *framework* organico e integrato, volto a garantire un bilanciamento tra promozione dell'innovazione tecnologica e tutela effettiva dei diritti delle persone danneggiate, con l'obiettivo di affiancare funzionalmente il regolamento sull'intelligenza artificiale, fornendo una cornice di riferimento per la responsabilità derivante da pregiudizi causati dall'utilizzo di sistemi di IA ad alto rischio. Tuttavia, nonostante la coerenza strutturale che tale proposta avrebbe potuto assicurare al *corpus* normativo emergente, la mancata convergenza tra gli Stati membri su un modello condiviso di disciplina della responsabilità extracontrattuale in ambito tecnologico – dovuta, in larga parte, alla difficoltà di conciliare approcci nazionali eterogenei in materia di onere della prova, presunzioni di colpa e criteri di imputabilità – ha determinato il definitivo accantonamento della proposta. Cfr. *Annexes to the ommunication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission work programme 2025*, COM(2025) 45 final.

informazioni relative alla sussistenza del nesso di causalità tra il funzionamento del prodotto (cd. " difettoso") e il danno cagionato [93].

La direttiva, pur avendo una portata generale, rappresenta un passo in avanti importante nel quadro normativo europeo volto a promuovere la diffusione dell'intelligenza artificiale in un'ottica di responsabilizzazione di coloro che ricorrono a tale tecnologia. L'individuazione di un soggetto responsabile assume un ruolo cruciale, poiché il ciclo di vita dei sistemi di IA coinvolge inevitabilmente una pluralità di attori, ciascuno con doveri specifici legati alla progettazione, alla manutenzione e alla gestione dei rischi connessi al loro utilizzo. L'obiettivo comune rimane quello di garantire la trasparenza, favorendo un bilanciamento tra l'innovazione tecnologica e la tutela dei diritti e degli interessi delle parti coinvolte.

3.2.1. *I sistemi di riconoscimento biometrico a distanza: per la prima volta uno schema normativo di riferimento*

Con il regolamento (UE) 2024/1689 è stato introdotto il primo quadro di regole per l'impiego dei sistemi di riconoscimento biometrico "a distanza" con l'esclusione, dunque, di tutti quei dispositivi che, per la raccolta o l'acquisizione dei dati, richiedono un contatto con un sensore o con un'interfaccia [94]. Vi rientrano pacificamente i sistemi di riconoscimento facciale che operano senza richiedere alcuna forma di collaborazione attiva o interazione da parte del soggetto interessato [95]. Tra questi, però, sono esclusi dall'ambito di applicazione i sistemi di verifica dell'identità che permettono di accedere a un servizio, sbloccare un dispositivo o disporre l'accesso di sicurezza a locali fisici [96]. Secondo il regolamento, l'utilizzo di questi strumenti presenta un impatto meno significativo sui diritti fondamentali rispetto ai sistemi di identificazione biometrica remota, i quali possono trattare dati personali di un numero elevato di individui [97]. Questo differente livello di intrusione deriva dal fatto che la finalità di verifica è generalmente circoscritta a contesti specifici e mirati, limitandosi a confermare l'identità di un individuo già noto al sistema.

---

[93] Cfr. l'art. 10.

[94] Art. 3, par. 1, n. 41. Cfr. il capitolo II, § 3.

[95] Cfr. il capitolo II, 2.1.

[96] Cfr. l'art. 3, par. 1, n. 36.

[97] Cfr. il considerando 17.

Nonostante l'apparente innocuità di tali applicazioni, il crescente ricorso ai metodi di verifica biometrica nei dispositivi commerciali pone rilevanti questioni sul piano giuridico. La registrazione sistematica dei *templates*, ovvero delle rappresentazioni digitali delle caratteristiche biometriche degli utenti per finalità di verifica, costituisce un'operazione quotidiana per le persone. L'esclusione normativa rischia di oscurare ancora di più le finalità per cui tali tecnologie operano, rendendo sempre meno accessibile la comprensione delle loro funzionalità e delle modalità di impiego. Questi dati, sebbene raccolti e utilizzati principalmente per finalità commerciali, potrebbero acquisire rilevanza anche per il *law enforcement*, offrendo elementi potenzialmente utili per le attività investigative e probatorie, con tutte le relative conseguenze connesse all'uso di *dati generati automaticamente* in un procedimento [98].

Tornando all'ambito di applicazione del regolamento, il documento ha adottato due discipline distinte: una per i sistemi di riconoscimento biometrico remoti in grado di operare in *tempo reale*, impiegati «in spazi accessibili al pubblico» [99], dalle autorità di *law enforcement* [100]; l'altra per gli strumenti che operano *a posteriori*, ovvero i sistemi in *real-time* impiegati per altre finalità [101], introducendo, per entrambe una nozione di riferimento.

Mentre i sistemi di riconoscimento *in tempo reale* sono gli strumenti tramite i quali «il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi» [102], la definizione dei sistemi che operano *a posteriori*, invece, viene individuata in via residuale: tra questi, rientrano gli strumenti di identificazione "a distanza" «diversi da un sistema

---

[98] Cfr. il capitolo III, § 4.1.

[99] Intendendosi per questi come «qualsiasi luogo fisico di proprietà pubblica o privata accessibile a un numero indeterminato di persone fisiche, indipendentemente dal fatto che possano applicarsi determinate condizioni di accesso e indipendentemente dalle potenziali restrizioni di capacità». Art. 3, par. 1, n. 44.

[100] Individuate tra «a) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse; oppure b) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse». Art. 3, par. 1, n. 45.

[101] Cfr. allegato III, par. 1, lett. a).

[102] Art. 3, par. 1, n. 42.

di identificazione biometrica remota in tempo reale» [103], e quindi, caratterizzati da uno scarto di tempo significativo intercorrente fra le fasi di comparazione e riconoscimento dei dati.

L'art. 5 elenca una serie di applicazioni a rischio "inaccettabile" e dunque, fatte salve alcune ipotesi eccezionali, vietate [104]. Per quel che rileva ai fini della presente trattazione, fra queste rientrano i sistemi di riconoscimento delle emozioni in contesti specifici [105] e la categorizzazione biometrica, in grado di classificare «individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale» [106]. L'impiego di questi strumenti, al fine di «*classifying people in public places as of a certain ethnicity or political orientation*», potrebbe rivelarsi particolarmente intrusivo per l'esercizio di alcune libertà fondamentali [107]. Per esempio, i risultati delle categorizzazioni potrebbero generare problematiche in termini di stigmatizzazione sociale,

---

[103] Art. 3, par. 1, n. 43.

[104] Tra queste si ricordano, i sistemi che sfruttano tecnologie subliminali per manipolare i comportamenti di una o più persone, quelli che sfruttano le vulnerabilità di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il comportamento in modo che ne provochi un danno significativo, nonché i sistemi di punteggio o cd. *social scoring*. Vengono annoverati altresì i sistemi di categorizzazione biometrica in grado di «trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale», con l'importante eccezione per l'utilizzo di dataset biometrici nel settore di *law enforcement* (art. 5, par. 1, lett. g); l'attività di «*scraping*» o, letteralmente «pesca a strascico» da internet di immagini dei volti (art. 5, par. 1, lett. e); infine, l'uso dei sistemi di riconoscimento delle emozioni nei luoghi di lavoro o negli istituti scolastici, anche in questo caso prevedendo un'eccezione per l'impiego «per motivi medici o di sicurezza» (art. 5, par. 1, lett. f).

[105] L'art. 5, par. 1, lett. f) prescrive il divieto per «l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza». Per un approfondimento, cfr. F.P. LEVANTINO-I.N. REZENDE, *Rischio inaccettabile: usi proibiti*, in O. POLLICINO-F. DONATI-G. FINOCCHIARO-F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, Giuffrè, Milano, 2025, p. 184 ss.

[106] Art. 5, par. 1, lett. g).

[107] Cfr. sul punto G. MALGIERI-M. IENCA, *The EU regulates AI but forgets to protect our mind*, 7 luglio 2021, reperibile su https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/.

soprattutto laddove l'attribuzione a specifiche categorie risulti pregiudizievole a causa di stereotipi consolidati in un determinato contesto socio-politico. L'associazione automatizzata a determinati gruppi può infatti amplificare fenomeni di marginalizzazione e consolidare pregiudizi esistenti, con effetti diretti sulla dignità e sull'identità sociale degli individui.

Il divieto posto dal regolamento, tuttavia, non si estende all'«etichettatura» o al «filtraggio di *set d*i dati biometrici» acquisiti legittimamente, sulla base di parametri biometrici o alla categorizzazione di tali dati nel contesto delle attività di *law enforcement.* In questi casi, i sistemi sono considerati ad "alto rischio" e occorre che si rendano conformi a una serie di condizioni e requisiti per il loro impiego ai sensi degli artt. 6 e seguenti [108].

3.2.2. *Gli strumenti di riconoscimento* in tempo reale

Tra gli impieghi a rischio "inaccettabile" compare anche il ricorso ai sistemi di identificazione biometrica *in tempo reale*, da parte di autorità di *law enforcement*, in spazi accessibili al pubblico [109], dal momento che «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» [110]. Il disposto del già citato art. 5, par. 1, lett. h) riguarda uno dei temi più dibattuti lungo il percorso che ha portato all'adozione del testo finale del regolamento.

A differenza di altre pratiche proibite elencate nell'art. 5, in questo caso il legislatore eurounitario ha avuto cura di specificare numerosi criteri e circostanze in cui l'impiego di questa tecnologia da parte delle autorità di *law*

---

[108] Tra questi si ricordano, la predisposizione di adeguati meccanismi di valutazione dei rischi, un'elevata qualità della serie di dati che alimentano il sistema per ridurre al minimo possibili risultati discriminatori, la registrazione dell'attività per garantire la tracciabilità dei risultati, la documentazione dettagliata che fornisca tutte le informazioni necessarie sullo scopo perseguito, le informazioni chiare e adeguate da fornire ai soggetti interessati, la predisposizione di adeguate misure di sorveglianza umana per ridurre al minimo il rischio di violazione di diritti fondamentali e un elevato livello di robustezza, sicurezza e precisione.

[109] Con "spazio accessibile al pubblico" s'intende «qualsiasi luogo fisico di proprietà pubblica o privata accessibile a un numero indeterminato di persone fisiche, indipendentemente dal fatto che possano applicarsi determinate condizioni di accesso e indipendentemente dalle potenziali restrizioni di capacità». Cfr. l'art. 3, n. 44 e considerando 19.

[110] Cfr. considerando 32; art. 5, par. 1, lett. h).

enforcement è consentito [111], purché sia «strettamente necessario per perseguire un interesse pubblico rilevante e la cui importanza prevale sui rischi» [112].

Le ipotesi eccezionali sono:

i) la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale, nonché la ricerca di persone scomparse;
ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico;
iii) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni.

Avendo già introdotto il tema entro la cornice delle garanzie fondamentali e dei rischi che ne possono derivare, sopra trattati [113], si può qui rivolgere l'attenzione a profili più specifici. Già ad una prima lettura, infatti, emergono alcuni dubbi legati alla potenziale frequenza con cui, in contesti caratterizzati da elevati assembramenti di persone – come eventi sportivi, concerti o raduni politici – si possa effettivamente configurare la minaccia qualificata come "sostanziale e imminente" dall'art. 5, lett. h). L'incertezza nasce dalla difficoltà di individuare un criterio oggettivo su una percezione, inevitabilmente soggettiva, come quella di un "pericolo" e richiama la necessità di definire casi standard condivisi, in grado di legittimare la richiesta di

[111] Ciascuno Stato potrà decidere se vietare *in toto* l'uso dei sistemi di identificazione biometrica *in tempo reale* sul proprio territorio, oppure prevedere l'impiego solo in relazione ad alcuni degli obiettivi previsti ai punti i-iii) dell'art. 5, lett. h). Il regolamento infatti lascia ai singoli ordinamenti la facoltà di decidere se attuare o meno le suddette eccezioni per l'impiego dei *tools* di riconoscimento tramite specifiche leggi nazionali. È escluso che l'art. 5, comma 1, lett. h) possa costituire la base giuridica per il trattamento di dati biometrici *ex* art. 10 dir. 2016/680. Cfr. il considerando 37, 2021/0106(COD). Per un approfondimento, cfr. C. PAPPALARDO, *L'identificazione biometrica remota*, in G. CASSANO-E.M. TRIPODI, *Il regolamento europeo sull'intelligenza artificiale. Commento al Reg. UE n. 1689/2024*, Maggioli, Santarcangelo di Romagna, 2024, p. 484.

[112] Cfr. il considerando 33. Il Parlamento europeo, in occasione della votazione plenaria del testo di compromesso aveva proposto di abolire le eccezioni e introdurre il divieto assoluto di impiego. Le tre ipotesi sono poi state reintrodotte in sede di triloghi.

[113] Cfr. il capitolo III.

eventuali misure. Soprattutto in situazioni caratterizzate da un rilevante afflusso di persone, il ricorso a dispositivi di identificazione biometrica (quali, ad esempio, i sistemi di riconoscimento facciale) solleva interrogativi stringenti sulla soglia oltre la quale l'adozione risulti giustificata. Il carattere indefinito della percezione di pericolo, spesso accentuato da fattori emotivi, non può costituire di per sé una motivazione sufficiente a legittimare interventi ad alto impatto sui diritti delle persone coinvolte.

Le medesime perplessità emergono in merito ai criteri da adottare per la corretta individuazione delle circostanze in cui sia possibile determinare, con un grado di certezza sufficiente, la presenza di una specifica vittima di reato o di una persona scomparsa (lett. h, i).

Anche la terza ipotesi (lett. h, iii) potrebbe rivelarsi di complessa applicazione, dal momento che la gravità del reato, che permette l'attivazione della tecnologia, è misurata in base al massimo della pena edittale prevista, che può essere diversa da Stato a Stato, per le stesse fattispecie di reato [114]. L'elenco comprende diversi delitti che vanno dal terrorismo al traffico di esseri umani, dagli abusi sessuali su minori e la pornografia minorile, al traffico di droghe e sostanze psicotrope, dai crimini ambientali alla partecipazione ad un'organizzazione criminale [115]. Le tipologie coinvolte risultano estremamente generiche e possono abbracciare anche ipotesi di gravità medio-bassa, comportando l'attivazione dello strumento *in tempo reale* anche in casi di indagine per reati minori [116].

---

[114] Il considerando 33 specifica che «l'elenco dei reati di cui all'allegato del presente regolamento è basato sui 32 reati elencati nella decisione quadro 2002/584/GAI del Consiglio, tenendo conto che alcuni reati risultano più pertinenti di altri, poiché il grado di necessità e proporzionalità del ricorso all'identificazione biometrica remota *in tempo reale* potrebbe essere prevedibilmente molto variabile per quanto concerne il perseguimento pratico della localizzazione o dell'identificazione nei confronti di un autore o un sospettato dei vari reati elencati e con riguardo alle possibili differenze in termini di gravità, probabilità e portata del danno o delle eventuali conseguenze negative».

[115] «Terrorismo, tratta di esseri umani, sfruttamento sessuale di minori e pornografia minorile, traffico illecito di stupefacenti o sostanze psicotrope, traffico illecito di armi, munizioni ed esplosivi, omicidio volontario, lesioni gravi, traffico illecito di organi e tessuti umani, traffico illecito di materie nucleari e radioattive, sequestro, detenzione illegale e presa di ostaggi, reati che rientrano nella competenza giurisdizionale della Corte penale internazionale, illecita cattura di aeromobile o nave, violenza sessuale, reato ambientale, rapina organizzata o a mano armata, sabotaggio, partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati elencati». Cfr. Allegato II del regolamento.

[116] Cfr. V.L. RAPOSO, *Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence*, in *IJLIT*, Vol. 30, Issue 1, 2022, p. 88-109.

In questa prospettiva, la disposizione, oltre a presentare profili di parziale collisione con il principio di proporzionalità [117], potrebbe portare a disparità di trattamento con conseguenti potenziali problematiche nell'ottica della cooperazione giudiziaria e di polizia. Infatti, potrebbe esserci il rischio che l'attivazione di tale strumento venga ammessa in uno Stato e non sia, per lo stesso fatto di reato, attivabile in un altro. Inoltre, nell'ipotesi in cui un'autorità giudiziaria formuli una richiesta di acquisizione probatoria fondata sull'utilizzo di un sistema di identificazione biometrica e tale strumento non sia previsto o disciplinato dalla normativa dello Stato richiesto, potrebbe sorgere un problema di mancata eseguibilità dell'atto o di divergente valutazione sulla legittimità della prova acquisita. La mancanza di armonizzazione, anche solo minima, in materia probatoria all'interno degli ordinamenti giuridici europei e internazionali amplifica la complessità di questo scenario [118]. La disomogeneità normativa tra i vari Stati membri genera incertezza sia in merito alle modalità di acquisizione della prova sia rispetto ai criteri di ammissibilità che devono essere rispettati affinché la prova raccolta all'estero possa essere impiegata nel processo interno.

L'art. 2 par. 3 stabilisce poi che il regolamento «non si applica a settori che non rientrano nell'ambito di applicazione del diritto dell'Unione e, in ogni caso, non pregiudica le competenze degli Stati membri in materia di *sicurezza nazionale*». Non essendo presente una definizione univoca e condivisa di "sicurezza nazionale" all'interno del quadro normativo europeo, la disposizione apre inevitabilmente la strada a interpretazioni ampie e potenzialmente arbitrarie da parte degli Stati membri, i quali mantengono una piena discrezionalità nell'individuare le situazioni rientranti in tale ambito. La conseguenza diretta di questa incertezza è l'aumento del rischio che la motivazione della sicurezza nazionale venga utilizzata come strumento giustificativo per l'adozione di misure invasive, come il ricorso al riconoscimento facciale *in tempo reale*, anche in contesti in cui tali tecnologie potrebbero non essere strettamente necessarie.

---

[117] Cfr. il capitolo III, § 4 ss.

[118] Cfr. per un approfondimento L. BACHMAIER WINTER-F. SALIMI (a cura di), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings. Electronic Evidence, Efficiency and Fair Trial Rights*, Hart Publishing, Dublin, 2024; R. BELFIORE, *Quali prospettive per l'ammissibilità reciproca delle prove fra gli Stati membri dell'Unione europea?*, in *Cass. pen.*, 2023, p. 3870; L. BACHMAIER WINTER, *Mutual Admissibility of Evidence and Electronic Evidence in the EU. A New Try for European Minimum Rules in Criminal Proceedings?*, in *Eucrim*, 2, 2023.

Passando all'analisi del successivo paragrafo dell'art. 5 (§ 2), gli strumenti *in tempo reale* possono essere attivati solo per «confermare l'identità della persona specificamente interessata», tenendo conto della «natura della situazione», delle «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*). L'indicazione secondo cui questi strumenti possono essere impiegati esclusivamente per «confermare l'identità» del destinatario della misura appare problematica [119]. Da una parte, viene esclusa ogni possibilità di utilizzo del sistema per identificare soggetti ignoti, confermando un approccio normativo volto a limitare rigorosamente l'impiego di tali tecnologie nel rispetto del principio di minimizzazione dei dati. Dall'altra, però, non può non rilevarsi una potenziale violazione della stretta necessità, secondo cui non dovrebbero essere impiegate quelle misure investigative che si limitano ad arricchire in maniera superflua un quadro ricostruttivo già adeguatamente delineato [120].

La *ratio* della norma potrebbe essere ricercata nel funzionamento tecnico del sistema *in tempo reale*, il quale presuppone, in ogni caso, un'operazione preliminare di individuazione dei profili nella *watchlist* [121]. Tale fase implica un'attività di filtraggio e selezione preventiva dei dati da parte degli operatori, i quali devono individuare i soggetti di interesse su cui concentrare l'analisi. Questa caratteristica strutturale del sistema determina sì un grado di discrezionalità nella composizione della banca dati di riferimento, ma rende il processo circoscritto a una rosa di individui selezionata (ciò consente di anticipare già qui una delle conclusioni cui giungerà il presente lavoro, ovvero la centralità della conoscenza delle modalità

[119] Art. 5, par. 2.

[120] «*The use of the expression 'confirming the identity', as opposed to 'identification', is meant as an additional safeguard for the fundamental rights limiting the risk of indiscriminate surveillance and implies that the identification of an individual within the meaning of Article 5(1)(h) AI Act must be targeted. That expression should be understood as meaning that the use of real-time RBI may only be initiated to search for specific individuals for which the law enforcement authorities have reasons to believe or are informed that they are victims of the crimes listed in Article 5(1)(h)(i) AI Act or are involved in one of the scenarios described in Article 5(1)(h)(ii) or Article 5(1)(h)(iii) AI Act. (…)*». Cfr. *Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689*, cit., p. 113.

[121] Cfr. il capitolo II, § 4.

di funzionamento tecnico dello strumento digitale che possono rappresentare il discrimine tra compatibilità o meno con i principi fondamentali dell'ordinamento).

Segue poi (§§ 3 e 4 dell'art. 5) l'onere in capo alle autorità di *law enforcement* di completare una valutazione d'impatto sui diritti fondamentali [122], una volta registrato il sistema in un'apposita banca dati, fatta eccezione per i casi di urgenza, «indicando contestualmente i motivi per cui non si è potuto richiederla prima, senza indebito ritardo e al più tardi entro 24 ore» [123]. Il riferimento ai sistemi non ancora registrati riguarda sia quelli che sono stati sviluppati e testati in condizioni reali, sia i cd. "*regulatory sandboxes*" [124], prima che gli stessi siano messi sul mercato.

In situazioni di urgenza operativa, dunque, la normativa prevede la possibilità di impiegare strumenti di identificazione biometrica anche in assenza di una valutazione d'impatto preventiva e senza l'obbligo di registrazione preliminare dei dati presso le apposite banche dati ufficiali. La deroga, sebbene giustificata dalla necessità di rispondere tempestivamente a esigenze di sicurezza o di ordine pubblico, solleva interrogativi critici circa la tenuta e la coerenza del quadro regolamentare. Consentire il ricorso a sistemi *in tempo reale* non ancora sottoposti a valutazione d'impatto, non registrati nell'apposita banca dati, e impiegati in contesti operativi "reali", potrebbe risultare poco coerente con gli obiettivi di tutela dei diritti fondamentali sanciti dallo stesso regolamento, generando un potenziale rischio di utilizzi non conformi o lesivi.

La disposizione prosegue poi prescrivendo l'obbligo di richiedere, per l'attivazione dello strumento, un'autorizzazione da parte di un'autorità giudiziaria o amministrativa indipendente, in conformità al diritto nazionale [125]. Il sistema può essere attivato, su istanza motivata, «sulla base di prove oggettive» e «indicazioni chiare» sulla necessità e sulla proporzionalità della misura agli obiettivi da perseguire [126]. A ulteriore garanzia, il quadro normativo specifica che nessuna decisione suscettibile di produrre effetti giuridici pregiudizievoli nei confronti di una persona, possa essere

---

[122] Cfr. A. MANTELERO, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template*, in *CLSR*, 2024, p. 54.

[123] Cfr. artt. 5, par. 1, lett. h), par. 2, 27 e considerando 34 e 96.

[124] Cfr. art. 3, par. 1, n. 53.

[125] Art. 5, par. 3.

[126] In casi di urgenza, l'autorizzazione può essere richiesta successivamente e senza indebito ritardo, al più tardi entro le 24 ore dall'impiego di questi strumenti, art. 5, par. 3.

assunta esclusivamente sulla base dell'*output* generato dal sistema [127]. La previsione dell'obbligo di richiedere un'autorizzazione è chiaramente tesa a garantire un adeguato livello di supervisione, promuovendo un controllo che possa limitare i rischi connessi all'uso improprio o arbitrario di tali strumenti. Tuttavia, la previsione normativa che consente agli Stati membri di designare, in via discrezionale, quale autorità competente per il rilascio dell'autorizzazione all'impiego dei sistemi di riconoscimento biometrico remoti *in tempo reale*, alternativamente un'autorità giudiziaria ovvero un'autorità amministrativa, solleva rilevanti perplessità sotto il profilo delle garanzie strutturali e funzionali di indipendenza e imparzialità della decisione autorizzativa. L'attribuzione di tale facoltà in capo al legislatore nazionale, in assenza di parametri vincolanti comuni, comporta il rischio di un ricorso a soluzioni eterogenee, non sempre rispettose dell'indipendenza istituzionale delle autorità [128].

L'opzione di affidare tale competenza, per esempio, a un'autorità requirente o a un'autorità amministrativa, prive delle stesse garanzie di indipendenza degli organi con funzioni giurisdizionali, infatti, potrebbe compromettere la neutralità del processo decisionale [129]. In particolare, le autorità amministrative, per loro natura legate all'apparato esecutivo, potrebbero – se non indipendenti – subire pressioni politiche o istituzionali che rischiano di influenzare la valutazione delle richieste di autorizzazione [130]. Al contrario, l'esclusivo affidamento di tale facoltà ad un giudice garantirebbe, almeno in

---

[127] Cfr. il capitolo III, § 4.1

[128] Cfr. I. BARKANE, *Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance*, in *Information Polity*, 27, 2022, p. 155; O. POLLICINO-F. PAOLUCCI, *I limiti all'attività di polizia: dati biometrici e genetici solo con il controllo del giudice*, in *Il Sole 24 Ore*, 17 dicembre 2024; F. PAOLUCCI, *From Global Standards to Local Safeguards: The AI Act, Biometrics, and Fundamental Rights*, in *SSRN*, 2024; F. PAOLUCCI, *The enforcement of the artificial intelligence act: looking forward to a commission implementing decisions for protecting fundamental rights*, in O. POLLICINO-F. DONATI-G. FINOCCHIARO-F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, Giuffrè, Milano, 2025, p. 356.

[129] Cfr. P. SCHÜTZ, *Assessing Formal Independence of Data Protection Authorities in a Comparative Perspective*, in J. CAMENISCH, *et al.* (eds.), *Privacy and Identity Management for Life. Privacy and Identity 2011. IFIP Advances in Information and Communication Technology*, vol 375, Springer, Berlin, Heidelberg, 2012.

[130] CGUE, *Commission v Poland*, C-530/16, 2018, ECLI:EU:C:2018:430, § 67: «*as regards public bodies*, *dependence usually refers to a status that ensures that the body in question is able to act completely freely in relation to those bodies in respect of which its independence is to be ensured, shielded from any instructions or pressure*».

linea teorica, un maggiore grado di indipendenza, essendo il suo operato soggetto a criteri e garanzie costituzionali che ne preservano l'autonomia rispetto agli altri poteri dello Stato. L'operato del giudice è vincolato dal principio del *giudice naturale precostituito per legge*, nonché da garanzie di irremovibilità e autonomia che consolidano il suo ruolo di terzietà rispetto alle parti del processo. Ciò si traduce in un controllo più incisivo sull'attivazione di misure invasive, tanto più rilevante nel contesto di strumenti tecnologici ad alto impatto sui diritti della persona.

Nel delineare il contenuto sostanziale del requisito di «autorità indipendente», risulta dirimente il contributo offerto dalla giurisprudenza della Corte di giustizia dell'Unione europea, in linea di continuità interpretativa con gli approdi della Corte europea dei diritti dell'uomo [131]. In tale contesto, l'indipendenza dell'autorità designata non si esaurisce in una garanzia formale di separazione dal potere esecutivo (cd. indipendenza esterna), ma deve essere altresì intesa nella sua accezione interna, quale manifestazione di imparzialità strutturale e funzionale, intesa come assenza di pregiudizi, vincoli o interessi nella risoluzione del caso concreto [132]. Sulla scorta di tali coordinate ermeneutiche, appare legittimo sollevare riserve circa la possibilità di considerare il pubblico ministero italiano quale soggetto pienamente conforme alla nozione autonoma di "autorità indipendente" ai sensi del diritto sovranazionale [133]. Benché il nostro ordinamento assicuri al pubblico ministero forme significative di autonomia rispetto al potere esecutivo [134] – superiori, in molti casi, a quelle previste in altri sistemi europei – e, seppur gravi sul pubblico ministero anche l'onere di cercare elementi a favore dell'accusato, permane il dato strutturale per cui esso resta parte processuale e portatore di una funzione d'accusa nel procedimento penale. Tale ruolo rende difficilmente compatibile la sua figura con un ideale di neutralità assoluta, richiesto per l'attribuzione di poteri autorizzativi in materia di restrizione

---

[131] Cfr. CGUE, 19 settembre 2006, *Graham J. Wilson contre Ordre des avocats du barreau du Luxembourg*, C-506/04, §§ 51-52 e, nell'ambito della Corte di Strasburgo, C. eur. 29 marzo 2010, *Medvedyev c. Francia*, n. 3394/03, § 124; C. eur. 23 novembre 2010, *Moulin c. Francia*, n. 37104/06, § 58.

[132] Cfr. CGUE, *Graham J. Wilson*, cit., § 52.

[133] Cfr. I. NERONI REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di data retention*, in *Sist. pen.*, 13 maggio 2020, p. 190 ss.

[134] La Corte di Cassazione ha ritenuto che la figura del pubblico ministero, per come disciplinata nell'ordinamento italiano, rappresenti un organo sufficientemente indipendente, cfr. Cass. pen., sez. III, 19 aprile 2019, n. 36380, con nota di I. NERONI REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di data retention*, cit., p. 188 ss.

dei diritti fondamentali, quali quelli implicati, ad esempio, dall'utilizzo di tecnologie biometriche o di sorveglianza avanzata [135].

Una volta ottenuta l'autorizzazione, il regolamento prescrive un obbligo di notifica all'autorità di vigilanza del mercato interno e all'autorità nazionale per la protezione dei dati di ciascun utilizzo di sistemi *in tempo reale* [136]. Sebbene la disposizione miri a garantire un controllo formale sull'impiego di questa tecnologia, solleva al contempo alcuni interrogativi circa l'effettività delle attività di verifica che le autorità sono chiamate a esercitare. L'obbligo di notifica, così come formulato, infatti, non chiarisce se tale adempimento si limiti a una comunicazione *ex post* dell'utilizzo dei sistemi o se, al contrario, implichi una valutazione preventiva circa la loro conformità ai principi di necessità, proporzionalità e minimizzazione dei dati, sanciti dalla normativa europea in materia di protezione dei dati personali. La mancanza di chiarezza normativa potrebbe indebolire l'effettività dei meccanismi di controllo, riducendoli a un mero esercizio formale privo di reale incisività.

A sua volta il paragrafo quinto dell'art. 5 specifica che gli Stati membri saranno liberi di prevedere la possibilità di autorizzare in tutto o in parte l'uso di sistemi *in tempo reale*, «nel proprio diritto nazionale e le necessarie regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni». In questa prospettiva, l'introduzione di disposizioni normative interne caratterizzate da livelli eterogenei di rigore regolativo rischia di compromettere l'effettiva armonizzazione delle prassi applicative in materia di riconoscimento biometrico, incidendo negativamente sulla coerenza e sull'efficacia del sistema europeo di *governance* dell'intelligenza artificiale. Tale disomogeneità potrebbe, per esempio, dar luogo a fenomeni di "*forum shopping* tecnologico" da parte di potenziali autori di reati, ovvero scenari in cui gli operatori del settore decidono di implementare sistemi biometrici negli Stati con regolamentazioni più permissive o meno strutturate.

Infine, il paragrafo 6 dell'art. 5 dispone che la Commissione europea pubblichi report annuali sul funzionamento dei sistemi di riconoscimento biometrico impiegati dalle forze di polizia, basandosi su dati aggregati forniti dalle autorità nazionali competenti in materia di protezione dei dati personali e di sorveglianza del mercato interno (par. 7). Sebbene questa previsione miri a garantire un livello minimo di trasparenza, la limitazione all'analisi dei

---

[135] Per un approfondimento sul tema cfr. F. PAOLUCCI, *The enforcement of the artificial intelligence act: looking forward to a commission implementing decisions for protecting fundamental rights*, cit., p. 359.

[136] Cfr. l'art. 5, § 4.

soli dati aggregati, senza un riferimento esplicito alle statistiche nazionali sottostanti, solleva dubbi in merito alla capacità di offrire una visione chiara e dettagliata sul reale utilizzo di tali strumenti. L'uso esclusivo di dati aggregati potrebbe ridurre significativamente la possibilità di valutare l'impatto reale di questi sistemi, nascondendo potenziali discrepanze o abusi nell'applicazione delle tecnologie biometriche a livello nazionale. La trasparenza, elemento essenziale per mantenere la fiducia dei cittadini, rischia così di essere compromessa in assenza di un resoconto più contestualizzato che permetta di comprendere non solo l'estensione dell'uso di tali sistemi, ma anche le specifiche circostanze operative, i risultati ottenuti e i potenziali errori o *bias* riscontrati.

Una maggiore attenzione alle statistiche nazionali sottostanti consentirebbe di evidenziare eventuali problematiche nell'implementazione dei sistemi biometrici, come disparità nell'accuratezza del riconoscimento per gruppi demografici diversi o un'applicazione non uniforme tra gli Stati membri. Ciò rappresenterebbe un passo fondamentale per garantire che tali strumenti siano utilizzati in modo proporzionato e conforme ai principi di legalità e necessità, evitando derive discriminatorie o distorsioni nell'impiego delle tecnologie da parte di governi con minori garanzie democratiche [137].

3.2.3. *Gli strumenti di riconoscimento* a posteriori

I sistemi biometrici *a posteriori* sono stati classificati come "ad alto rischio", considerato che «le inesattezze di carattere tecnico (…) possono determinare risultati distorti e comportare effetti discriminatori» [138]; tuttavia, restano consentiti. Il regolamento ha previsto infatti una disciplina più "attenuata" per questa modalità applicativa, posto che il ricorso ad essa sarebbe meno intrusivo rispetto ai sistemi impiegati *in tempo reale* dalle autorità di *law enforcement* in spazi accessibili al pubblico [139].

---

[137] Cfr. i capitoli V, § 5 e VI, § 1.

[138] Cfr. considerando 32. Entro la stessa categoria rientrano anche i sistemi di riconoscimento biometrico *in tempo reale* e quelli di categorizzazione non vietati dall'art. 5.

[139] Cfr. EDPB-GEPD, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale)*, 18 giugno 2021, p. 13; A. SCHRÖDER, *"Real-time" versus "post" remote biometric identification systems under the AI Act*, ALTI Forum, 14 ottobre 2022. Si veda su questo punto più ampiamente il capitolo III, § 2.

Per tutti i sistemi "ad alto rischio", i requisiti da rispettare sono quelli previsti dagli artt. 6 ss., ossia la predisposizione di adeguati meccanismi di valutazione e mitigazione dei rischi, la registrazione dell'attività per garantire la tracciabilità dei risultati, la documentazione dettagliata che fornisca tutte le informazioni necessarie sullo scopo perseguito, le informazioni chiare e adeguate da fornire ai soggetti interessati, la predisposizione di misure di sorveglianza umana per ridurre al minimo il rischio di violazione di diritti fondamentali e un elevato livello di robustezza, sicurezza e precisione [140].

Poiché nella modalità *a posteriori* il confronto biometrico, qualora non siano applicati specifici filtri di ricerca dall'operatore, può avvenire con l'intera banca dati [141], risulta imprescindibile l'adozione di rigorosi criteri di gestione dei dati per garantire l'affidabilità e l'efficacia del sistema. In particolare, la normativa richiede che i *set* di dati utilizzati nelle fasi di addestramento e convalida degli strumenti siano sottoposti a pratiche di gestione avanzate che assicurino la loro pertinenza, rappresentatività, accuratezza ed esaustività. In tal senso, la selezione del *dataset* deve tener conto delle peculiarità del contesto geografico e funzionale entro cui la tecnologia è impiegata, così da assicurare che i modelli siano adeguatamente tarati sulle specifiche condizioni operative [142]. Tuttavia, pur essendo concettualmente auspicabile, il raggiungimento di una completa neutralità dei dati rappresenta un obiettivo difficile da realizzare, soprattutto nei sistemi biometrici già esistenti e operativi su larga scala. La raccolta dei dati risulta soggetta a variazioni qualitative legate a fattori ambientali (come la qualità delle immagini o le condizioni di illuminazione), tecnologici (come l'affidabilità dei sensori) o umani (errori nell'acquisizione o nella registrazione dei dati) [143].

A ciò si aggiungono le sfide economiche e organizzative associate all'aggiornamento e alla ricostruzione di sistemi biometrici già esistenti. Il processo di adeguamento dei *dataset* ai requisiti di completezza, accuratezza e rappresentatività richiede non solo un significativo sforzo tecnico, ma anche ingenti risorse finanziarie. La creazione *ex novo* di database conformi o

---

[140] Per un approfondimento sui criteri e sui sistemi ad alto rischio, R. RODRIGUEZ DE LAS HERAS BALLELL, *High risk AI systems in the European AI Act*, in O. POLLICINO-F. DONATI-G. FINOCCHIARO-F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, Giuffrè, Milano, 2025, p. 246.

[141] Cfr. il capitolo II, § 4.

[142] Cfr. il considerando 67.

[143] Cfr. il capitolo II, § 4.6.

l'adeguamento di quelli esistenti comportano costi elevati e complessità operative che spesso limitano la possibilità di effettuare aggiornamenti tempestivi e completi.

Anche per i sistemi di riconoscimento biometrico *a posteriori* viene espressamente previsto l'obbligo di ottenere un'autorizzazione preventiva, da richiedersi *ex ante* o, in casi di urgenza, senza indebito ritardo entro 48 ore, da parte di un'autorità giudiziaria o amministrativa indipendente [144]. L'atto è poi sottoposto a controllo giurisdizionale per verificare la legittimità e la stretta necessità rispetto alle finalità perseguite, in particolare per garantire che l'uso del sistema sia finalizzato esclusivamente a indagini su reati specifici e gravi [145], escludendo quindi applicazioni generalizzate o indiscriminate e che non si traduca in un aggiramento delle restrizioni rigorose imposte al divieto di identificazione biometrica remota *in tempo reale* [146]. La previsione di un provvedimento autorizzativo è volta a garantire altresì che «nessuna decisione che produca effetti giuridici negativi su una persona, possa essere presa dalle autorità di contrasto unicamente sulla base dell'*output* di tali sistemi di identificazione biometrica remota a posteriori» [147]. Qualora l'autorizzazione richiesta venga rigettata, l'impiego del *tool* deve essere immediatamente interrotto. Tale sospensione assume effetto immediato e vincolante, al fine di prevenire ogni ulteriore trattamento dei dati biometrici raccolti in assenza di una legittimazione formale da parte dell'autorità competente [148].

La norma si differenzia parzialmente da quella stabilita per gli strumenti *in tempo reale* [149], dal momento che richiede espressamente un controllo giurisdizionale, rafforzando così l'indipendenza e l'imparzialità del provvedimento adottato. Tuttavia, la disciplina ammette un'eccezione significativa: non è richiesta un provvedimento preventivo quando il sistema è impiegato

---

[144] Art. 26, par. 10.

[145] «In nessun caso tale sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori è utilizzato a fini di contrasto in modo non mirato, senza alcun collegamento con un reato, un procedimento penale, una minaccia reale e attuale o reale e prevedibile di un reato o la ricerca di una determinata persona scomparsa». Art. 26, par. 10.

[146] Art. 26, par. 10 e il considerando 95.

[147] Art. 26, par. 10. Cfr. il capitolo III, § 4.1.

[148] A seguito della revoca, è imposto l'obbligo di procedere alla cancellazione integrale dei dati personali acquisiti tramite l'utilizzo del sistema per il quale era stata richiesta l'autorizzazione.

[149] Art. 5, par. 3.

per l'identificazione iniziale di un potenziale sospettato, a condizione che tale attività si basi su fatti oggettivi e verificabili, direttamente connessi al reato oggetto di indagine [150]. Questa eccezione, pur volta a garantire l'efficienza investigativa in situazioni di urgenza, solleva questioni critiche sotto il profilo delle garanzie procedurali. Si ritiene infatti che debba rimanere fermo il fatto che i risultati ottenuti attraverso tale identificazione possano essere utilizzati esclusivamente a fini di identificazione nella fase preliminare e non deve essere consentito il loro impiego anche in fasi successive. Il rischio principale risiede nel fatto che l'assenza di limiti chiari potrebbe consentire un riutilizzo dei dati biometrici anche in fasi successive del procedimento, senza che sia stata adeguatamente osservata la riserva di giurisdizione o che siano state adottate le adeguate garanzie difensive [151].

Infine, per entrambe le modalità, viene prevista una sorveglianza umana rafforzata, attraverso una procedura di verifica obbligatoria dell'*output* generato dal sistema, da parte di almeno due operatori indipendenti [152]. L'introduzione del doppio controllo umano assume una valenza cruciale non solo per ridurre al minimo gli errori sistemici, ma anche per attenuare l'impatto di potenziali *bias* algoritmici o di condizionamenti cognitivi che potrebbero influenzare il giudizio di un singolo operatore.

La disposizione normativa, però, contempla ancora una volta una deroga significativa per i sistemi impiegati per fini di *law enforcement*, prevedendo che la misura del doppio controllo possa essere omessa in considerazione delle esigenze operative e della necessità di interventi tempestivi in contesti di pubblica sicurezza. In questo modo, l'esonero dal doppio controllo umano, soprattutto nei contesti di *law enforcement*, rischia di amplificare le incertezze connesse a decisioni automatizzate non adeguatamente verificate.

3.2.4. *Alcune prime brevi riflessioni sul regolamento*

Alla luce di tutto quanto sopra esposto, il regolamento non risulta privo di incertezze interpretative. Il testo normativo è caratterizzato da un uso significativo di termini vaghi e concettualmente ridondanti, privi, nella maggior parte dei casi, di definizioni esplicative o chiarimenti adeguati.

---

[150] Art. 26, par. 10.

[151] Cfr. il capitolo V, § 4.

[152] Cfr. il considerando 73.

Tale carenza terminologica incide negativamente sulla chiarezza e sulla precisione del quadro regolamentare, generando incertezze applicative che rischiano di compromettere la coerenza e l'uniformità di attuazione delle disposizioni.

L'assenza di definizioni normative dettagliate comporta, inoltre, un ampio margine di discrezionalità, che finisce per essere affidato, in prima istanza, ai soggetti privati direttamente coinvolti nell'attuazione del regolamento, quali i fornitori di tecnologie e gli operatori responsabili della messa in funzione e dell'utilizzo pratico dei sistemi. Questa situazione attribuisce a tali soggetti una rilevante autonomia decisionale, con il rischio di generare prassi non uniformi e potenzialmente divergenti rispetto agli obiettivi di tutela perseguiti dal legislatore.

I principali dubbi che emergono riguardano la portata applicativa di alcune disposizioni contenute nel documento come sopra descritto: in particolare, sarà interessante comprendere come le diverse eccezioni al divieto di riconoscimento *in tempo reale* da parte delle autorità di *law enforcement*, in spazi accessibili al pubblico, opereranno in concreto nei vari Stati membri e come l'interpretazione generale del regolamento ne verrà di riflesso condizionata.

Il dato positivo è rappresentato dall'inserimento di norme minime che gli Stati membri dovranno implementare, anche inserendone di nuove e più specifiche, adattando il regolamento ai vari sistemi giuridici nazionali.

Il rischio di frammentazione normativa, però, appare elevato, soprattutto in assenza di un intervento tempestivo e coordinato da parte degli organi istituzionalmente deputati all'attuazione del regolamento [153], che potrebbe condurre a una proliferazione di prassi interpretative e applicative eterogenee tra i diversi Stati membri, compromettendo l'obiettivo di uniformità e coerenza che il quadro regolamentare europeo intende perseguire. Considerando la base legale e la struttura della fonte esaminata, gli adempimenti più gravosi saranno certamente richiesti agli sviluppatori dei sistemi di IA, che dovranno dimostrare la conformità ai diversi requisiti descritti, dalla quale il regolamento fa dipendere la tutela dei diritti fondamentali coinvolti, oltre che la garanzia del buon funzionamento del mercato interno.

Sul piano della tecnica normativa, il quadro delineato prevede significative eccezioni ai divieti generali di utilizzo dei sistemi di intelligenza artificiale, introducendo deroghe appositamente formulate per consentirne

[153] Cfr. F.P. LEVANTINO-I.N. REZENDE, *Rischio inaccettabile: usi proibiti*, in O. POLLICINO-F. DONATI-G. FINOCCHIARO-F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, Giuffrè, Milano, 2025, p. 196.

l'impiego nell'ambito delle attività tradizionalmente connesse all'indagine e alla repressione dei reati. Sebbene tali deroghe siano giustificate dall'obiettivo di garantire l'efficienza operativa e l'efficacia delle attività investigative, per come risultano genericamente formulate, esse sollevano molteplici interrogativi in merito alla loro compatibilità con alcune garanzie fondamentali. In questa prospettiva, i principi generali sanciti dall'ordinamento giuridico operano come contrappesi volti a bilanciare l'impiego di tali strumenti tecnologici con la salvaguardia dei diritti e delle libertà fondamentali. È essenziale, pertanto, che tali eccezioni siano accompagnate da un rigoroso sistema di controllo e da misure adeguate a prevenire abusi e a garantire un'applicazione conforme ai valori fondamentali di uno Stato democratico.

4. *Le ricadute sulla cooperazione di polizia e gli sviluppi del sistema di scambio e di circolazione dei dati*

Le disposizioni analizzate delineano il quadro giuridico di riferimento per l'impiego delle tecnologie di riconoscimento biometrico a distanza, configurandosi come cornice normativa trasversale, applicabile ai molteplici ambiti e settori nei quali tali sistemi trovano impiego. In tale prospettiva, il regolamento sull'intelligenza artificiale assume il ruolo di *lex generalis*, fornendo i principi fondamentali su cui si innesta qualsiasi ulteriore normativa di settore. A questo proposito, in parallelo e in un'ottica di rafforzamento della cooperazione transnazionale in materia di sicurezza, il legislatore europeo ha adottato il regolamento (UE) 2024/982 ("*Prüm II*"), inerente la consultazione e lo scambio automatizzati di dati per la cooperazione di polizia, che ha innovato il sistema istituito con il Trattato di Prüm [154], il quale, a sua

[154] Il sistema introdotto con il Trattato di Prüm ha avuto l'obiettivo di favorire lo scambio su larga scala si impronte digitali, profili ricavati dal DNA e dati di immatricolazione dei veicoli a scopi di polizia e sicurezza nazionali. Sottoscritto il 27 maggio 2005 dal Regno del Belgio, dalla Repubblica federale di Germania, dal Regno di Spagna, dalla Repubblica francese, dal Granducato di Lussemburgo, dal Regno dei Paesi Bassi e dalla Repubblica d'Austria e relativo all'attuazione della cooperazione transfrontaliera, in particolare allo scopo di contrastare il terrorismo, la criminalità transfrontaliera e la migrazione illegale. Il sistema istituito dal Trattato di Prüm costituisce un esempio di cooperazione "rafforzata" realizzata esternamente alla

volta, ha avuto lo scopo di rafforzare il coordinamento tra gli Stati nella lotta al terrorismo, alla criminalità transfrontaliera e all'immigrazione illegale, tramite alcune specifiche aree di intervento: a) la raccolta e lo scambio di informazioni relative ai profili del DNA; b) la raccolta e lo scambio di informazioni sulle impronte digitali; c) lo scambio dei dati relativi ai registri di immatricolazione dei veicoli; d) le misure finalizzate a prevenire reati terroristici ed, infine, e) le misure dirette a contrastare l'immigrazione illegale [155].

A pochi anni di distanza, sono state approvate le decisioni 2008/615/GAI e 2008/616/GAI che hanno pienamente integrato il Trattato di Prüm nell'ambito del quadro normativo europeo. La prima, finalizzata a migliorare lo scambio di informazioni, in un'ottica di cooperazione, prevede che gli Stati membri si concedano reciprocamente l'accesso ai rispettivi schedari automatizzati di analisi del DNA, ai sistemi automatizzati di identificazione dattiloscopica e ai dati di immatricolazione dei veicoli.

In particolare, il meccanismo di cooperazione si basa su un sistema "*hit/no hit*", che consente allo Stato membro che effettua la consultazione in uno schedario automatizzato di chiedere allo Stato membro che lo gestisce i dati personali specifici corrispondenti e, se necessario, ulteriori informazioni mediante procedure di assistenza reciproca [156]. Per i dati concernenti i profili del DNA e le impronte digitali, il sistema Prüm ha predisposto un meccanismo di accesso online ai soli dati di indice. Questi ultimi contengono solamente la parte di DNA non codificante o i dati dattiloscopici con un generico riferimento, ma non consentono l'identificazione diretta di un individuo. In questo modo, nel caso in cui, a seguito di una consultazione automatizzata dei dati, fosse riscontrabile una concordanza, gli Stati interessati sarebbero posti nelle condizioni di richiedere poi il dato completo, al fine di compiere le analisi necessarie. La

---

cornice comunitaria. Successivamente, con la decisione 2008/615/GAI il Trattato è stato incorporato nel quadro giuridico dell'Unione europea. È stato ratificato dall'Italia con la legge 30 giugno 2009, n. 85, prevedendo l'istituzione della Banca dati nazionale del DNA e la disciplina del prelievo e del trattamento dei campioni biologici (cfr. il capitolo II, § 4.2).

[155] Occorre tenere distinti i sistemi centralizzati, quali SIS, VIS, EURODAC, SID, Europol, Eurojust e i sistemi decentralizzati, come quello istituito dal Trattato di Prüm. I primi sono strutturati in database gestiti a livello centralizzato e in *network* che pongono in collegamento istituzioni e organismi dell'UE e i vari Stati membri. Per un approfondimento cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, p. 248 ss.

[156] Cfr. il considerando 10 della decisione 2008/615/GAI del Consiglio, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera.

trasmissione dei dati personali e delle informazioni ulteriori è conforme «al diritto nazionale della Parte contraente richiesta, comprese le disposizioni relative alla collaborazione giudiziaria» (artt. 5 e 10 della decisione n. 615).

La seconda decisione si concentra sul potenziamento della cooperazione internazionale, con particolare riferimento alle strategie di contrasto al terrorismo e alla criminalità transfrontaliera. In questo contesto, il principio di disponibilità assume un ruolo determinante nel facilitare il processo di condivisione delle informazioni tra gli Stati membri, consentendo un più rapido ed efficiente accesso ai dati rilevanti per le attività investigative e giudiziarie. L'applicazione di questo principio mira a superare le tradizionali barriere burocratiche e giuridiche che spesso ostacolano lo scambio di informazioni tra le autorità competenti di diversi ordinamenti.

Un elemento di inciampo era rappresentato dalla diversa operatività delle banche dati nazionali e dal grado di interconnessione tra i database dei diversi Stati membri. La mancanza di un sistema di coordinamento omogeneo per l'accesso e la gestione dei dati biometrici e personali ha spinto le istituzioni europee a riflettere sulla necessità di riformare il meccanismo esistente, al fine di renderlo più efficace e meno esposto a criticità di carattere giuridico e operativo.

Per far fronte alle difficoltà operative e alla frammentarietà del quadro giuridico di riferimento, unitamente all'affermarsi di nuove tecniche e strumenti di indagine basati sul trattamento di dati personali, le istituzioni dell'Unione europea, in particolare la Commissione e il Consiglio, hanno cominciato a promuovere iniziative legislative [157], studi e ricerche concernenti la modernizzazione delle decisioni di Prüm e del relativo meccanismo di scambio dei dati [158]. Tra queste iniziative, spicca il regolamento sullo scambio

---

[157] Cfr. regolamento (UE) 2024/982 del Parlamento europeo e del Consiglio del 13 marzo 2024 sulla consultazione e lo scambio automatizzati di dati per la cooperazione di polizia e 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 (regolamento «*Prüm II*»).

[158] L'espressione "*Next generation Prüm*" è stata coniata dal *Working Party on Information Exchange and Data Protection*, un organo preparatorio del Consiglio, che ha iniziato a vagliare la possibilità di dar seguito al progetto in esame. Cfr. WORKING PARTY ON INFORMATION EXCHANGE AND DATA PROTECTION (DAPIX), 4 aprile 2017, reperibile su https://www.consilium.europa.eu/en/meetings/mpo/2017/4/working-party-on-information-exchange-and-data-protection-dapix-(255033)/. Per un primo commento sul tema V.L. SCAFFARDI, *Next Generation Prüm e le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, in *federalismi.it*, 8, 2021, p. 211 ss., L.

automatizzato di dati per la cooperazione di polizia ("*Prüm II*"), che ha modificato 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.

Basandosi sulle procedure esistenti per la consultazione automatizzata dei dati, la novità più importante del documento normativo consiste proprio nella possibilità di inserire, insieme ai profili del DNA, ai dati dattiloscopici e a quelli relativi ai veicoli immatricolati, anche i dati relativi ai casellari giudiziari e le rappresentazioni digitalizzate dei volti, finalizzate all'impiego di sistemi automatici di riconoscimento facciale [159]. Introducendo la previsione di una consultazione e uno scambio transfrontaliero di immagini facciali [160], si rende possibile eseguire un riconoscimento biometrico impiegando informazioni contenute nelle banche dati di altri Stati membri.

Il primo obiettivo della normativa consiste nella creazione di banche dati nazionali contenenti le rappresentazioni digitali dei volti, analogamente a quanto stabilito dalle decisioni di Prüm per altre categorie di dati. Gli archivi sono gestiti in modo autonomo da ciascuno Stato membro e devono contenere i dati biometrici sia di soggetti ignoti, sia di soggetti condannati o ricercati e, dunque, già noti alle autorità di *law enforcement.*

Il regolamento prevede la creazione di due *sistemi centrali* (il Prüm II e il sistema europeo di indicizzazione dei casellari giudiziari – EPRIS), punto di connessione tra i vari Stati membri. Si tratta di un approccio ibrido tra una soluzione decentrata e una centralizzata, senza alcuna archiviazione di dati a livello centrale.

Ciò implica che le banche dati nazionali in ciascuno Stato membro comunichino tramite il *router* centrale, anziché connettersi tra di loro. Tale *router* fungerebbe da intermediario di messaggi, inoltrando le operazioni di consultazione e le risposte ai sistemi nazionali, senza creare nuove elaborazioni di dati o ampliare i diritti di accesso, né sostituire le banche dati nazionali.

SCAFFARDI, *Forensic genetics: The evolving challenge of DNA cross-border exchange*, in *Riv. BioDir.*, Special Issue 1(2021), p. 329 ss., e H. MACHADO-R. GRANJA-A. AMORIM, *Ethical challenges of merging criminal identification and civil identification within the Prüm system*, in *Forensic Science International: Genetics*, 57, 2022.

[159] Cfr. COMMISSIONE EUROPEA, DIREZIONE GENERALE DELLA MIGRAZIONE E DEGLI AFFARI INTERNI, *Study on the feasibility of improving information exchange under the Prüm decisions: cost benefits analysis: final version*, Publications Office, 2020.

[160] Cfr. l'art. 4, par. 10 che chiarisce che per "immagine facciale" debba intendersi «l'immagine digitalizzata del volto».

Il modello di cooperazione proposto ricalca quello avente ad oggetto le altre tipologie di dati: a una prima trasmissione dell'immagine di un volto alle autorità competenti individuate da ciascuno Stato membro, seguirebbe l'esecuzione di un'operazione di comparazione sulla base del meccanismo *hit/no hit.* Nel caso di esito positivo, viene data esecuzione al trasferimento e alla condivisione delle informazioni personali dell'individuo da parte dello Stato membro, il cui database contenga una immagine facciale che corrisponda a quella inoltrata dal Paese richiedente. In caso di corrispondenza tra i dati utilizzati per la ricerca o il confronto e i dati conservati nella banca dati nazionale dello Stato richiesto, e previa conferma di tale corrispondenza da parte del richiedente, lo Stato membro richiesto dovrebbe trasmettere una serie limitata di dati di base tramite il *router* entro 24 ore. Lo scambio delle rappresentazioni digitali o di *templates* di volti dovrebbe avvenire sulla base di una serie di linee guida, introdotte per garantire la qualità standard delle immagini da scambiare [161], predisponendo un numero minimo e massimo di *matches* da trasferire e comunicare, e fissando termini brevi per la conservazione dei dati inviati per i quali non è stata riscontrata alcuna corrispondenza [162].

Dall'introduzione del regolamento però sono emerse non poche perplessità per la realizzazione pratica degli obiettivi perseguiti dal testo normativo.

In primo luogo, occorre evidenziare che la maggior parte degli Stati membri non dispone, allo stato attuale, delle infrastrutture tecniche né delle competenze operative necessarie per implementare in modo efficace e sistematico lo scambio transfrontaliero di dati biometrici facciali. Tale carenza riguarda sia la disponibilità di piattaforme interoperabili adeguatamente sicure e conformi agli standard previsti dalla normativa eurounitaria, sia la mancanza di protocolli condivisi che disciplinino in modo uniforme i criteri di acquisizione, conservazione, elaborazione e trasmissione delle immagini facciali digitalizzate.

A ciò si aggiungono criticità ulteriori che incidono direttamente sull'affidabilità degli strumenti di riconoscimento facciale. Un primo profilo riguarda la qualità spesso insufficiente delle immagini condivise tra i diversi

---

[161] Cfr. il considerando 21 *bis* e l'art. 23 *bis.* È inoltre previsto che *lo Stato membro richiedente dopo aver ricevuto un elenco di corrispondenze relativo ai possibili candidati, provveda affinché sia condotta una verifica da parte di due esperti forensi al fine di stabilire l'esistenza di una corrispondenza confermata (art. 22, par. 2).*

[162] Cfr. L. SCAFFARDI, *Next Generation Prüm e le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, cit., p. 217.

archivi nazionali e di quelle originariamente inserite nei database. Bassa risoluzione, angolazione non ottimale, scarsa illuminazione o distorsioni legate ai dispositivi di acquisizione possono compromettere in modo significativo l'efficacia dei confronti biometrico-automatizzati, aumentando esponenzialmente il rischio di falsi positivi o falsi negativi.

Un secondo e più strutturale profilo di rischio riguarda i modelli algoritmici su cui si fondano le operazioni di comparazione. Tali modelli, in assenza di un rigoroso processo di validazione indipendente, possono essere affetti da *bias* sistemici – riconducibili sia alla composizione non rappresentativa dei *dataset* di addestramento, sia a scelte progettuali – che determinano un trattamento diseguale tra diversi gruppi di soggetti. Ciò risulta particolarmente preoccupante nel contesto di un sistema europeo di scambio di dati, in cui un errore derivante da *bias* algoritmico potrebbe avere effetti a catena su più ordinamenti giuridici, compromettendo la fiducia reciproca tra autorità e, soprattutto, l'effettività delle garanzie dei diritti fondamentali [163]. Come è stato evidenziato, «*the degree of accuracy in facial recognition technology is vital, so as to minimise the risk of false positive matches, namely results that may be unrelated to the investigation, or false negative results, when the FR algorithm fails to identify correct matches. This is crucial since facial recognition technology will be used in the course of criminal investigations with the aim of identifying unknown perpetrators, therefore national authorities will perform searchers on the basis of a facial image (a mug shot or a probe retrieved from a camera) against the full content of other national databases and the top results will be ranked. False positive matches in particular may have important consequences for individuals, who may be bothered by the police because of incorrect matching, be subject to criminal investigation and even be subject to discriminatory practices by national authorities*» [164].

Pertanto, pur riconoscendo che l'intervento umano rappresenti, anche in questo contesto, un presidio imprescindibile a garanzia dell'affidabilità e della correttezza del risultato prodotto dal sistema algoritmico, non possono non emergere significative perplessità in ordine all'effettiva efficacia di tale assetto tecnico-procedurale. La previsione di una supervisione umana – volta a confermare o smentire le corrispondenze individuate automaticamente dal

---

[163] Cfr. EDPS, *Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation ("Prüm II")*, 2 marzo 2022, p. 6.

[164] Cfr. POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS OF THE EUROPEAN PARLIAMENT, *Police Information Exchange – The future developments regarding Prüm and the API Directive*, 15 settembre 2020, p. 32.

software – costituisce certamente un elemento di rafforzamento in termini di controllo e verifica, volto a mitigare i rischi di errori o falsi positivi. Tuttavia, permane il dubbio sulla concreta utilità dell'integrazione delle rappresentazioni digitalizzate dei volti nel quadro del meccanismo Prüm, rispetto ai risultati effettivamente conseguibili in termini di incremento dell'efficienza investigativa e cooperazione transfrontaliera. L'implementazione dello scambio automatizzato di immagini facciali, per quanto innovativa sul piano tecnologico, solleva dunque diversi interrogativi in merito al valore aggiunto che tale funzionalità apporterebbe al sistema, soprattutto in presenza di problematiche non ancora risolte, quali appunto l'eterogeneità nella qualità delle immagini, la disomogeneità dei *dataset* biometrici nazionali e l'assenza, in molti Stati membri, delle necessarie capacità infrastrutturali e operative [165].

Infine, il regolamento non sarebbe chiaro rispetto all'individuazione di specifiche fattispecie di reato per cui gli agenti di polizia potrebbero attivare il meccanismo di scambio, né con riferimento alle categorie di soggetti cui appartengono i dati che alimentano i database dei vari Stati membri [166]. Secondo l'EDPS [167], il documento «*should be further developed for what concerns the safeguards for fundamental rights of the data subjects in the case of exchange of facial images*» e, più nel dettaglio, eseguendo «*a distinction between different categories of data subjects, only the facial images of convicted criminals and suspects should be made available for queries* […] *the automated searching of facial images must be limited only to individual investigations of serious crimes, and not for any criminal offence, as provided for in the proposal*».

Nonostante l'adozione formale del regolamento, il dibattito dottrinale e istituzionale sulla legittimità e l'opportunità di tali previsioni rimane tuttora

---

[165] Cfr. POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS OF THE EUROPEAN PARLIAMENT, *Police Information Exchange – The future developments regarding Prüm and the API Directive*, 15 settembre 2020, cit., p. 33, «*contemporary research demonstrates that such searches are likely difficult due to an adequate quality of such images. If this option goes forward, the sources of facial images require clarity and data protection safeguards must be embedded so that the quality of facial images is high enough to prevent the risk of increased false matches, which may lead to discriminatory practices. The specific purposes for searching facial images should also be circumscribed so as to prevent wide-ranging surveillance practices at the national level*».

[166] Cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation ("Prüm II")*, p. 2.

[167] Cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation ("Prüm II")*, p. 11.

aperto e particolarmente vivace. Si è ancora in una fase embrionale rispetto alla concreta applicazione del nuovo assetto regolatorio, il che rende prematuro formulare previsioni attendibili in ordine agli effetti operativi che potranno derivarne e all'impatto che tale innovazione potrà esercitare sulla cooperazione transfrontaliera in materia di giustizia penale e pubblica sicurezza. La maggiore preoccupazione è rappresentata dall'assenza di una disciplina più dettagliata di riferimento e dai potenziali rischi correlati all'impiego di strumenti ritenuti «ancora dai contorni opachi e per certi aspetti controversi e criticati» [168].

[168] Cfr. L. SCAFFARDI, *Next Generation Prüm e le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, cit., p. 223.

Capitolo V

La comparazione automatizzata fra volti nell'attuale assetto codicistico

SOMMARIO: 1. Alla ricerca delle adeguate coordinate processuali. – 2. L'acquisizione dei volti a fini di comparazione. – 3. La rappresentazione digitalizzata del volto entro il *genus* della "prova digitale". – 4. La modalità applicativa *a posteriori*: nuovo trattamento o nuovo metodo? – 4.1. Il riconoscimento *a posteriori* e la categoria della prova atipica. – 4.1.1. Il requisito della libertà morale. – 5. La modalità applicativa *in tempo reale*. – 6. La capacità dimostrativa di un *match* biometrico. – 6.1. L'attendibilità del *match* biometrico. – 6.1.1. Il ruolo del calcolo del rapporto di verosimiglianza.

1. *Alla ricerca delle adeguate coordinate processuali*

Come già dimostrato, il "decreto capienze" si è rivelato uno strumento inadatto per la regolamentazione dei casi e delle modalità di ricorso ai sistemi di riconoscimento facciale. Sebbene esso abbia rappresentato un primo passo verso la messa a punto di una disciplina organica per l'uso di questa tecnologia nel settore di *law enforcement*, l'atto non offre previsioni esaustive, né criteri applicativi chiari. Le scarne disposizioni, infatti, consentono ai magistrati di ricorrere a questi strumenti di riconoscimento, ma omettono di tipizzare i casi di applicazione nonché di distinguere tra modalità e finalità conseguibili da questi sistemi.

A sua volta, come noto, il regolamento (UE) 2024/1689 ha introdotto una cornice normativa finalizzata, non solo a regolare l'accesso al mercato unico, ma anche a orientare i legislatori nazionali nell'impiego delle tecnologie basate sull'intelligenza artificiale. Tuttavia, le disposizioni contenute in tale documento non costituiscono la base normativa per il trattamento dei dati biometrici, così come richiesta dall'art. 10 della direttiva (UE) 2016/680 (considerando 38 del regolamento 2024/1689 che ribadisce l'applicabilità della direttiva). Come visto nel capitolo precedente, spetta ai singoli Stati membri

predisporre internamente una disciplina dettagliata per l'uso di sistemi di riconoscimento biometrico, nel rispetto dei principi sanciti dalla normativa europea in materia di protezione dei dati personali.

Anche il legislatore italiano dunque dovrà confrontarsi con tali obblighi. L'attuale situazione interna, però, fotografa uno scenario complesso che si può così riassumere: a) progressiva entrata in vigore di un regolamento che – come appena visto – non costituisce base normativa per il trattamento del dato biometrico e che impone agli Stati di introdurre una disciplina consonante; b) vigenza di una legge ordinaria nazionale, precedente al regolamento e non di settore, che non può essere disapplicata a favore del regolamento – per via delle ricordate caratteristiche di quest'ultimo – e che dunque costituisce parametro normativo di riferimento, sebbene come sopra ampiamente argomentato (cfr. i cap. III-IV), non paia né dotata dei requisiti espressamente previsti dagli artt. 13 Cost., 7, 8 e 52 CDFUE, 10 LED, che si ritengono principi che presidiano la disciplina qui in esame, né idonea ad implementare in maniera specifica le indicazioni del regolamento. In attesa dunque di veder superata l'attuale normativa, connotata da così tanti limiti, è interessante indagare se, nello specifico quadro normativo processuale interno, siano rinvenibili istituti idonei a offrire una funzione di supplenza per l'impiego di questi strumenti, individuandone le possibili collocazioni sistematiche [1]. Tale ricognizione assume rilevanza non solo sul piano pratico, ma anche sotto il profilo concettuale, poiché sollecita una rielaborazione dei paradigmi tradizionali del diritto processuale penale. L'analisi si fa ancor più significativa proprio perché potrebbe offrire le coordinate idonee – innanzitutto come ponte interpretativo verso le previsioni del regolamento (UE) 2024/1689 – a sistematizzare il precario e disordinato telaio normativo appena descritto.

Lo sforzo è parimenti teso a intercettare eventuali lacune che potrebbero ostacolare un'applicazione conforme alle garanzie fondamentali, al fine di delineare, almeno nei loro tratti essenziali, i caratteri che una futura

---

[1] Sul tema si segnalano G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*, in *Cass. pen.*, 2, 2025, p. 638; A. MARANDOLA, *Il riconoscimento facciale*, in C. CONTI-A. MARANDOLA, *La prova scientifica*, Giuffrè, Milano, 2023, p. 500 ss., nonché J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. e proc. pen.*, 2022, p. 41 ss.; volendo, E. SACCHETTO, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *Leg. pen.*, 16 ottobre 2020 e E. SACCHETTO, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Dir. pen. cont.-Riv. trim.*, 2, 2019.

disciplina dovrebbe presentare per garantire un bilanciamento tra le esigenze di efficienza investigativa e processuale e il rispetto dei diritti fondamentali coinvolti.

Non si può tuttavia volgere lo sguardo alla disciplina codicistica senza aver prima ribadito che la normativa *extra codicem* in materia di protezione dei dati personali, al momento non fornisce indicazioni specifiche (come invece accade per esempio in relazione all'acquisizione di tabulati telefonici)[2] circa l'utilizzabilità processuale delle prove acquisite tramite algoritmi di intelligenza artificiale, come quelle derivanti dai sistemi di riconoscimento facciale[3]. Questo scenario riflette una mancanza di coordinamento tra il legislatore in materia di privacy e quello processuale, i cui approcci normativi raramente procedono su binari destinati a convergere. Tale disallineamento genera una contraddizione interna nell'ordinamento giuridico, in cui un'attività può essere ritenuta legittima per determinati scopi, ma non per altri. Tuttavia, come previsto dall'art. 160-*bis*, inserito nel d.lgs. 30 giugno 2003, n. 196 (c.d. "codice della privacy") dal d.lgs. 10 agosto 2018, n. 10, «la validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali».

È allora nelle previsioni del codice di procedura penale che si devono individuare i criteri per valutare l'utilizzabilità e l'attendibilità della prova basata su modelli di intelligenza artificiale, come quella in oggetto. Il riferimento alle norme processuali consente infatti di stabilire se tali strumenti probatori, per loro natura complessi e altamente tecnici, soddisfino i requisiti di ammissibilità nel contesto del procedimento penale, garantendo il rispetto dei principi di legalità, contraddittorio e falsificazione.

Siamo in presenza di un insieme variegato di questioni, saldamente connesse alla specifica tematica delle "prove tecnico-scientifiche"[4], la quale

---

[2] Cfr. il d.l. 30 settembre 2021 n. 132, convertito in legge, con modificazioni, dall'art. 1, comma 1, legge 23 novembre 2021, n. 178.

[3] Cfr. M. TORRE, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. e proc.*, 8, 2021.

[4] La prova scientifica è intesa come «quella prova che, partendo da un fatto dimostrato, utilizza una legge scientifica per accertare l'esistenza di un ulteriore fatto da provare». P. TONINI-C. CONTI, *Il diritto delle prove penali*, Giuffrè, Milano, 2014, p. 354. Così, la scientificità sembra poter essere riconducibile, piuttosto, al risultato probatorio e, più precisamente, al giudizio inferenziale del giudice, cui è imposto di impiegare «conoscenze che vanno oltre

implica l'ottenimento di elementi conoscitivi acquisiti attraverso l'ausilio di strumenti tecnici, la cui capacità dimostrativa rispetto all'accertamento dei fatti oggetto di prova non può ancora darsi per scontata nel contesto culturale di riferimento, quantomeno rispetto al suo impiego in ambito giudiziario[5].

Preliminarmente, occorre riprendere alcune distinzioni cruciali, richiamando la scansione dei diversi passaggi del procedimento di riconoscimento. Il percorso di analisi prenderà così l'abbrivio dalle molteplici attività di reperimento delle tre categorie di dato biometrico, *trasformato/convertito, ricavato* e *generato automaticamente*[6]: dalla fase di reperimento all'acquisizione, sino al momento in cui il dato assume la forma di una rappresentazione digitalizzata, nel nostro caso del volto, ovvero, del suo modello biometrico. Tale percorso, oltre a delineare il progressivo trattamento dell'informazione biometrica, consente di inquadrarne la natura giuridica, verificando se e in che misura essa possa essere sussunta entro le maglie della consolidata

---

il sapere dell'uomo medio». Cfr. V. DENTI, *Scientificità della prova e libera valutazione del giudice*, in *Riv. dir. proc.*, 1972, p. 414 ss.; G. DI PAOLO, *"Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione*, Cedam, Padova, 2008, p. 8, sottolinea come entro la locuzione "prova tecnico-scientifica" possa essere ricondotta una molteplicità di fenomeni assai diversi tra loro, come per esempio «la ricerca della prova nella fase investigativa attraverso le cd. tecnologie del controllo; l'introduzione della prova nel processo attraverso l'impiego di mezzi tecnologici sofisticati; il formarsi della prova (qui intesa come risultato) attraverso un giudizio di inferenza probatoria che rende necessario integrare il patrimonio conoscitivo dell'organo giudicante con conoscenze specialistiche pertinenti al mondo della scienza e della tecnica (…)». Nel novero degli strumenti scientifico-tecnici, parte della dottrina distingue fra quelli che sono già oggetto di un'esperienza consolidata e condivisa nell'uso giudiziario e quelli "nuovi o controversi e di elevata specializzazione". Anche gli strumenti tecnico-scientifici consueti, come ad esempio, la rilevazione e l'analisi delle impronte digitali possono vedersi sopraggiungere da nuove formulazioni che li pongono in discussione, fino a renderli ad un certo punto problematici. O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, cit., p. 13. Cfr. F. FOCARDI, *La consulenza tecnica extraperitale delle parti private*, Cedam, Padova, 2003, p. 185 ss. in cui l'Autore evidenzia come la distinzione tra scienza ordinaria e *novel science*, pur certamente chiara in astratto, sia in realtà assai "sfuggente" in concreto, dal momento che non sarebbero stati specificati le concrete modalità e i soggetti che possono avanzare una richiesta di prova qualificata come di "scienza nuova". Cfr. ancora G. UBERTIS, *Il giudice, la scienza e la prova*, in *Cass. pen.*, 11, 2011; F. CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processso penale*, in *Cass. pen.*, 9, 2008; O. DOMINIONI, *In tema di nuova prova scientifica*, in *Dir. pen. e proc.*, 2001, p. 1061.

[5] Cfr. P. RIVELLO, *Tecniche scientifiche e processo penale*, in *Cass. pen.*, 4, 2013, p. 1691 ss.

[6] Cfr. il capitolo II, § 5.

categoria della prova digitale. A questo punto, si concentrerà l'attenzione sul *match,* considerando le diversità delle due modalità operative di confronto, *a posteriori* e *in tempo reale*[7]. In entrambi i casi, l'inquadramento giuridico del riconoscimento facciale varia in funzione della specifica finalità per cui lo strumento viene impiegato, rendendo necessaria una riflessione sui profili di compatibilità con le tradizionali categorie probatorie.

Ancora. Occorrerà poi confrontarsi con la capacità dimostrativa del risultato di un confronto biometrico fra i dati che non può prescindere dallo studio delle caratteristiche intrinseche del volto. La scarsa "riferibilità individualizzante", la limitata "permanenza" e l'elevata "variabilità" dovuta a fattori fisiologici, ambientali e tecnologici influenzano inevitabilmente il funzionamento degli strumenti di riconoscimento facciale[8], imponendo una riflessione critica sull'idoneità del contributo a ricostruire i fatti oggetto di prova nel contesto processuale e sulla necessità di mettere a punto adeguati meccanismi di controllo e validazione del dato.

2. *L'acquisizione dei volti a fini di comparazione*

La ricostruzione di un *iter* univoco di reperimento e acquisizione dell'informazione biometrica costituisce un'operazione alquanto complessa, poiché i passaggi variano in funzione della finalità perseguita e della tipologia di informazione considerata[9]. La diversità degli scenari applicativi incide significativamente sulle modalità di acquisizione, conservazione ed elaborazione del dato, rendendo necessario un approccio analitico che tenga conto delle specifiche tecnologie impiegate e dei contesti normativi di riferimento. Ciò impone di riprendere e approfondire concetti già in vario modo introdotti che, altrimenti, rischierebbero di rimanere inafferrabili.

La variabilità del percorso probatorio del dato biometrico rappresenta una specifica declinazione del tema che si ritiene opportuno riprendere e calare nello scenario procedimentale. La fase in cui vengono – nella maggior parte dei casi – acquisite le immagini, da cui sono individuati ed estratti i volti, coincide con le indagini preliminari. Invero, molto spesso il maggiore

[7] Cfr. il capitolo II, § 4.

[8] Cfr. il capitolo II, § 4.6.

[9] Cfr. il capitolo II, § 5.

ricorso a strumenti tecnologici si registra proprio nella fase investigativa iniziale [10], laddove la polizia giudiziaria, il pubblico ministero e i consulenti tecnici si avvalgono di strumenti di elevata specializzazione e di conoscenze scientifiche di ultima elaborazione [11].

Attraverso l'impiego di software, ai quali sempre più di frequente sono applicate tecniche di IA, in grado di riconoscere soggetti o captare segretamente flussi di conversazioni, scambi telematici e dati digitali di diversa natura, gli organi inquirenti dispongono di un'amplissima gamma di azioni a tratti estremamente intrusive, sconosciute fino a pochi anni fa. Ma non solo. Da molti dispositivi digitali, anche quelli aventi finalità del tutto estranee al procedimento penale, è possibile estrarre molteplici informazioni di rilievo per le indagini [12]. La posizione degli oggetti all'interno di un ambiente domestico può influenzare il comportamento di dispositivi automatizzati, come nel caso di un'aspirapolvere intelligente che adatta il proprio percorso in funzione degli ostacoli rilevati, consentendo così di inferire la disposizione spaziale di un ambiente in un determinato momento [13]. Analogamente, la rilevazione della presenza di un numero significativo di persone in una stanza,

---

[10] Sul punto si veda *ex multis* T. ALESCI, *Il corpo umano come fonte di prova*, Wolters Kluwer Cedam, Milano, 2017, p. 44; D. CURTOTTI-L. SARAVO, *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze, logica*, Torino, Giappichelli, 2019, p. 13, in A. SCALFATI (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2019; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 205 ss.; S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2, 2015, p. 760 ss.; F. CASASOLE, *Le indagini tecnico-scientifiche: un connubio tra scienza e diritto in perdurante attesa di disciplina*, in *Dir. pen. e proc.*, 11, 2008, p. 1443; R.V.O. VALLI, *Le indagini scientifiche nel procedimento penale*, in E. STEFANI (a cura di), *Il processo penale accusatorio*, Giuffrè, Milano, 2013, p. 756 ss.

[11] F. CASASOLE, *Le indagini tecnico-scientifiche*, cit., p. 1443 ss. e S. SMYTH, *Biometrics, surveillance and the law. Societies of restricted access, discipline and control*, Routledge, New York, 2019, p. 65, la quale afferma che «*law enforcement can be seen as the birthplace of biometrics*». Giova peraltro specificare che la polizia, procedendo anche ad atti a valenza tecnico-scientifica, può servirsi delle proprie strutture specializzate o di esperti esterni. Come è stato evidenziato, non è del tutto chiaro però se le «persone idonee» menzionate nell'art. 348 c.p.p. debbano intendersi come esperti esterni alle strutture di polizia (per es. un laboratorio pubblico di analisi) ovvero come esperti interni (per es. la divisione di polizia scientifica). Per una lettura critica del punto cfr. B. LAVARINI, *Elementi di procedura penale. Lezioni per il corso di laurea magistrale in chimica clinica, forense e dello sport*, ECIG, Genova, 2009, p. 119 ss.

[12] Cfr. il capitolo II, § 5.

[13] Cfr. S. QUATTROCOLO, *Giustizia penale e intelligenza artificiale: finestre su uno scenario da esplorare*, in A. PAJNO-F. DONATI-A. PERRUCCI, *Intelligenza artificiale e diritto: una rivoluzione?*, il Mulino, Bologna, 2022, p. 533-540.

determinabile attraverso l'aumento della temperatura e l'attivazione automatica di sistemi di climatizzazione o di raffreddamento, offre un dato oggettivo che può essere utilizzato per ricostruire la dinamica di specifici eventi [14]. *Face ID* di Apple e i sistemi equivalenti sui dispositivi Android, inizialmente sviluppati per garantire un accesso sicuro ai dispositivi mobili, si sono progressivamente evoluti, introducendo funzionalità avanzate come l'analisi delle espressioni facciali per una maggiore sicurezza e personalizzazione dell'esperienza utente.

Sono molteplici le apparecchiature che, sulla base di modelli di intelligenza artificiale, sono in grado di svolgere azioni non già su impulso meccanico di un utente, ma a partire dall'analisi dei dati raccolti, da cui deriva l'*input* per agire [15]. La categoria è quella dei *dati generati automaticamente* [16]: in questo caso, le informazioni vengono elaborate al fine di estrarre correlazioni e generare autonomamente un *output* [17]. Sebbene il modello biometrico memorizzato nel dispositivo costituisca il risultato di un processo di elaborazione algoritmica, non necessariamente comprensibile o accessibile in modo diretto da parte delle autorità inquirenti [18], la rappresentazione digitale delle caratteristiche biometriche dell'individuo, una volta registrata nel dispositivo, si configura come un elemento informativo potenzialmente idoneo a contribuire all'accertamento dei fatti di reato. Per esempio, i sistemi di videocitofonia intelligenti integrati con algoritmi di riconoscimento, non

---

[14] Cfr. S. QUATTROCOLO, *Giustizia penale e intelligenza artificiale: finestre su uno scenario da esplorare*, cit., p. 533.

[15] Cfr. R. LEENES-S. DE CONCA, *Artificial intelligence and privacy. Ai enters the house through the cloud*, in W. BARFIELD-U. PAGALLO, *Research Handbook on the Law of Artificial Intelligence*, Edward Elgar publishing, Cheltenham-Northampton, 2018, p. 295.

[16] Cfr. il capitolo II, § 4 ove si richiama la classificazione operata da S. QUATTROCOLO, *Equità del processo penale e a*utomated evidence *alla luce della Convenzione europea dei diritti dell'uomo*, in *Revista Italo-Española de Derecho Procesal*, 2019, p. 2 ss. Cfr. anche C. CESARI, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, Porto Alegre, 5(3), 2019, p. 1169.

[17] Cfr. S. BARONA VILAR, *Una jusiticia 'digital' y 'algoritmica' para una sociedad en stado de mudanza*, in S. BARONA VILAR (a cura di), *Justicia algoritmica y neuroderecho*, Tirant Lo Blanch, Valencia, 2021, p. 26 ss.

[18] Cfr. A. RATTANI-R. DERAKHSHANI, *A Survey Of mobile face biometrics*, in *Computers & Electrical Engineering*, Vol. 72, November 2018, p. 39-52; R. RAMACHANDRA-M. STOKKENES-A. MOHAMMADI-S. VENKATESH-K. RAJA-P. WASNIK-E. POIRET-S. MARCEL-C. BUSCH, *Smartphone Multi-modal Biometric Authentication: Database and Evaluation*, in *Journal of latex class files*, 14(8), 2015.

si limitano a registrare passivamente le immagini, ma elaborano *in tempo reale* le informazioni biometriche acquisite tramite sensori visivi per confrontarle con modelli biometrici precedentemente archiviati nel dispositivo. Il loro funzionamento si basa sulla generazione automatica del dato: la telecamera, infatti, rileva l'ingresso di un individuo all'interno del perimetro visivo, estrae le caratteristiche morfologiche del volto e le confronta con la *watchlist* interna, contenente le rappresentazioni digitali dei volti associati a soggetti autorizzati. L'intero processo si svolge in modo autonomo, senza che sia richiesto l'intervento umano, e culmina nella produzione automatica di un *output* – ad esempio, l'apertura del varco di accesso, l'invio di un *alert* o la registrazione dell'evento nel *log* di sistema – sulla base della corrispondenza rilevata. Il *template* biometrico immagazzinato nel sistema costituisce il risultato di un processo algoritmico che, sebbene operativamente efficace, può risultare non immediatamente interpretabile o accessibile da parte dell'autorità giudiziaria, a causa della natura opaca delle tecniche impiegate. Nonostante ciò, laddove venga accertato che il dispositivo abbia effettuato correttamente un'associazione tra il volto di un soggetto e un evento delittuoso, il dato biometrico generato automaticamente e successivamente estratto potrebbe assumere una rilevanza probatoria.

In questo contesto, è bene tenere presente che l'accesso ai dati conservati in un dispositivo digitale costituisce, secondo consolidata giurisprudenza interna ed eurounitaria, una forma di ingerenza particolarmente intrusiva dei diritti fondamentali della persona interessata [19]. La rilevanza di tale interferenza deriva dalla natura intrinsecamente sensibile dei dati digitali presenti in tali dispositivi, i quali possono includere non solo contenuti comunicativi (quali messaggi di testo, e-mail, immagini o cronologie di navigazione), ma anche metadati capaci di ricostruire con estrema precisione il profilo esistenziale del soggetto: luoghi frequentati, relazioni sociali e professionali, abitudini quotidiane, orientamenti personali, preferenze politiche o religiose.

In ragione di tale carattere pervasivo, il legislatore nazionale ha recentemente proposto un intervento di riforma volto a disciplinare espressamente, all'interno del codice di procedura penale, le modalità di sequestro e di analisi dei dati contenuti in dispositivi e sistemi digitali [20]. In particolare, il

---

[19] Cfr. il capitolo III; *ex multis* CGUE, 4 ottobre 2024, C-548/21, Corte cost. n. 170/2023 con nota di L. FILIPPI, *Il cellulare "contenitore" di corrispondenza anche se già letta dal destinatario*, in *Riv. pen. dir. e proc.*, 2023. Per un approfondimento, K. LA REGINA, *Il sequestro dei dispositivi di archiviazione digitale*, in *Riv. pen. dir. e proc.*, 2023, p. 429.

[20] In seguito alla ratifica della Convenzione di Budapest sulla criminalità informatica

disegno di legge A.S. n. 806 introduce l'art. 254-*ter* c.p.p., intitolato "*Sequestro di dispositivi, sistemi informatici o telematici o memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute*" [21]. Muovendo dall'interpretazione di alcune pronunce giurisprudenziali sul tema, la proposta normativa si fonda sull'assunto secondo cui il sequestro di dispositivi informatici, in particolare di *smartphone* e computer,

(legge n. 48/2008 di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno), l'ordinamento italiano ha introdotto significative modifiche al codice di procedura penale, volte a disciplinare più puntualmente l'acquisizione probatoria di contenuti digitali. Tuttavia, l'art. 253 c.p.p., che disciplina il sequestro probatorio, non è stato oggetto di revisione, continuando a presentare rilevanti profili di criticità in relazione alla sequestrabilità del dato informatico. L'assenza di un adeguamento normativo di tale disposizione appare oggi particolarmente problematica, sia sotto il profilo sistematico che operativo, soprattutto in considerazione della crescente centralità che l'informazione digitale riveste nelle moderne attività investigative. La disciplina attualmente vigente, elaborata in un contesto tecnologico profondamente diverso da quello attuale, si fonda su una concezione materiale e tangibile dell'oggetto del sequestro, mal adattandosi alle peculiarità immateriali, duplicabili e facilmente alterabili del dato informatico. Tale lacuna normativa risulta oggi particolarmente significativa alla luce della crescente centralità dei dati informatici nelle attività investigative, sollevando questioni complesse sul piano della tipizzazione dell'oggetto del sequestro, nonché sull'adeguatezza delle garanzie previste per i tradizionali atti di acquisizione probatoria.

[21] La novella prevede un procedimento articolato, fondato su una scansione temporale e funzionale ben definita. In una prima fase, il giudice per le indagini preliminari, su istanza del pubblico ministero, può autorizzare il sequestro del dispositivo, purché ciò risulti necessario alla prosecuzione delle indagini e nel rispetto del principio di proporzionalità. Entro cinque giorni dal deposito del verbale di sequestro, il pubblico ministero conferisce l'incarico per la duplicazione del contenuto informatico del dispositivo, realizzando così un'immagine forense, ossia una copia integrale destinata all'analisi investigativa. Sulla base della successiva analisi tecnica del duplicato, il pubblico ministero, con decreto motivato, procede al sequestro selettivo dei soli dati "strettamente pertinenti" al fatto di reato, nel rispetto dei criteri di stretta necessità e proporzionalità, in riferimento alle specifiche circostanze temporali, spaziali e modali della condotta criminosa. Tuttavia, qualora l'oggetto del sequestro ricomprenda anche dati comunicativi – ossia dati riconducibili a conversazioni private o corrispondenza – si richiede un'autonoma autorizzazione giudiziale, secondo i parametri normativi e le condizioni sostanziali previste dagli artt. 266 e 267 c.p.p., che regolano le intercettazioni. Per un approfondimento sul tema cfr. "Modifiche al codice di procedura penale in materia di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali", www.senato.it. Cfr. O. MURRO, *Sequestro dei dispositivi informatici: verso l'art. 254 ter c.p.p.? Brevi note a margine del d.d.l. A.S. N. 806*, in *Riv. pen. dir. e proc.*, 12 marzo 2024 e O. MURRO, *Lo smartphone come fonte di prova. Dal sequestro del dispositivo all'analisi dei dati*, Wolters Kluwer Cedam, Milano, 2024.

debba essere sottoposto a un regime di garanzie assimilabile, per rigore e tutela, a quello previsto per le intercettazioni di comunicazioni [22]. L'attuale prassi operativa in materia di acquisizione di contenuti di dispositivi digitali, infatti, si caratterizza per una preliminare apprensione dell'intero sistema oggetto d'interesse investigativo, realizzabile secondo due modalità tecniche: da un lato, mediante la duplicazione forense del sistema informatico direttamente in sede di esecuzione del provvedimento ablativo; dall'altro, attraverso la materiale acquisizione delle memorie digitali, successivamente sottoposte a duplicazione in ambiente laboratoriale, al fine di procedere alla selezione dei dati rilevanti ai fini probatori [23]. Tale procedura, pur rispondendo all'esigenza di garantire la conservazione dell'integrità del dato, solleva significative criticità sul piano della tutela della riservatezza e dei diritti fondamentali della persona sottoposta a indagine. In particolare, la possibilità per gli organi inquirenti di accedere all'intero contenuto informativo del dispositivo – potenzialmente contenente dati del tutto estranei all'oggetto del procedimento – si traduce in un'inevitabile esposizione a un rischio di acquisizione eccedente, non proporzionata rispetto alle finalità perseguite [24].

I dati, poi, possono essere contenuti in supporti cartacei e venire trasposti, dagli esperti forensi, da strumenti analogici a digitali [25], ovvero potrebbero essere soggetti a particolari trattamenti tecnici [26], al fine di poter

---

[22] Cfr. *ex multis* Cass. pen., S.U., 19 aprile 2018, n. 36072, in *CED Cass.*, n. 273549, Cass. pen., sez. VI, 24 febbraio 2015, n. 24617, in *CED Cass.*, n. 264094.

[23] Cfr. il § successivo; *ex multis* Cass. pen., sez. VI, 22 settembre 2020, n. 34265, in *CED Cass*., n. 279949; Cass. pen., sez. II, 23 marzo 2023, n. 17604, in *CED Cass*., n. 284393; Cass. pen., sez. III, 4 luglio 2024, n. 36776, in *CED Cass.*, n. 286923. Per un approfondimento cfr. A. TESTAGUZZA, *Digital forensics. Informatica giuridica e processo penale*, Wolters Kluwer Cedam, Milano, 2015, p. 33 ss.; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 2015 ss.; M. PITTIRUTI, *Digital Evidence e procedimento penale*, Giappichelli, Torino, 2017, p. 33 ss.

[24] Per un approfondimento cfr. *ex multis* M. PITTIRUTI, *Dalla Corte di cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus*, in *Sist. pen.*, 14 gennaio 2021; L. BARTOLI, *Parità delle armi e discovery digitale: qualche indicazione da Strasburgo*, in *Leg. pen.*, 13 gennaio 2022; S. DE FLAMMEIS, *Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale*, in *Sist. pen.*, 8 marzo 2024.

[25] Un dato grezzo può subire un procedimento di digitalizzazione da parte degli organi inquirenti a fini di comparazione con altri modelli elettronici della stessa tipologia di dato (cd. "*dato trasformato/convertito*").

[26] Basti pensare al trattamento di un filmato di videosorveglianza dal quale è possibile

compiere delle comparazioni con altri *templates*, contenuti in ampi archivi di dati o in dispositivi digitali. Anche in questo caso, l'accesso alle informazioni ivi racchiuse può rappresentare per gli organi inquirenti una risorsa fondamentale, soprattutto nelle fasi preliminari delle indagini, fornendo elementi essenziali per orientare e indirizzare la ricerca di ulteriori spunti probatori. In questa prospettiva, si è fatto cenno alla categoria dei *dati trasformati o convertiti*[27]: le immagini rilevanti ai fini del riconoscimento possono derivare da documenti analogici extraprocedimentali oppure da un procedimento di *enrollment* biometrico di dati tramite appositi sensori o interfacce[28]. Una volta acquisiti, i dati sono sottoposti a un trattamento tecnico che può comprendere operazioni di elaborazione volte a ottimizzarne la qualità e a incrementarne l'idoneità all'analisi automatizzata. Tali interventi mirano a garantire la massima fruibilità del dato nell'ambito delle attività investigative, assicurandone la leggibilità, l'integrità e la compatibilità con le metodologie di comparazione automatizzata. L'attività di conversione/trasformazione parrebbe rientrare nell'ambito degli atti tecnici ripetibili *ex* art. 359 c.p.p., nella misura in cui essa non comporti un'alterazione irreversibile del dato originario e consente, almeno in astratto, una rinnovazione dell'operazione mediante gli stessi strumenti o tecniche equivalenti. Rimane fermo che la concreta ripetibilità di tali attività risulta condizionata da variabili tecniche, quali la qualità del supporto di origine, le condizioni di acquisizione e la configurazione del software utilizzato, che potrebbero incidere sulla coincidenza del risultato in sede di eventuale replica. In alternativa, e forse con maggiore aderenza al dato positivo, l'attività in parola potrebbe essere qualificata come atto atipico di assicurazione della fonte di prova, ai sensi della combinazione degli artt. 55 e 348 c.p.p. In questa prospettiva, la polizia giudiziaria, nell'ambito delle sue funzioni di iniziativa investigativa, svolgerebbe una operazione tecnico-ricognitiva finalizzata alla conservazione e alla valorizzazione di elementi potenzialmente rilevanti per il successivo accertamento giudiziale.

Infine, con riferimento alla categoria dei *dati ricavati*, la fonte primaria di acquisizione è rappresentata dalla ripresa video con la quale s'intende la «captazione di immagini, occulta o palese, effettuata mediante strumenti

---

ritagliare dei *frames* raffiguranti i tratti somatici di un individuo dai quali, a loro volta, ricavare le *features* per la creazione del modello elettronico biometrico o semplicemente per la rappresentazione digitale delle stesse.

[27] Cfr. il capitolo II, § 5.

[28] Cfr. il capitolo II, § 4.

tecnici che consentono di imprimere le stesse su un supporto in grado di riprodurle»[29]. Il segnale video è costituito da un insieme di immagini che, se riprodotte in successione, formano una sequenza di fotogrammi denominati *frames*[30]. Questi dati possono essere memorizzati localmente o trasmessi in rete, rendendo possibile la loro elaborazione, analisi e utilizzo per diverse finalità, tra cui il riconoscimento biometrico facciale. La configurazione digitale del segnale video consente l'applicazione di avanzati processi di compressione ed elaborazione, i quali ne potenziano l'efficienza operativa e ne ampliano le possibilità di utilizzo, sia in ambito investigativo che in contesti probatori. Tali caratteristiche permettono un trattamento ottimizzato del dato visivo, garantendo una maggiore affidabilità, integrità e interoperabilità con strumenti analitici avanzati, essenziali per l'estrazione di informazioni rilevanti ai fini dell'attività forense.

A fronte della diffusione sempre più crescente dell'uso di impianti di videosorveglianza, l'ordinamento ha risposto con una regolamentazione settoriale differenziata tra il settore pubblico e privato. A una disciplina piuttosto corposa sull'uso degli impianti di videosorveglianza per finalità di sicurezza pubblica[31], fa da contraltare l'assenza di un regime processuale organico in grado di assicurare un impiego probatorio certo e garantito delle riprese video all'interno del processo penale. In mancanza di un quadro normativo, infatti, è stata la giurisprudenza a delineare i limiti e le condizioni di legittimità dell'acquisizione e dell'utilizzabilità delle registrazioni nel circuito processuale, contribuendo a definire i parametri entro cui tali evidenze possono assumere rilevanza[32]. Come noto, l'interpretazione delle

---

[29] Cfr. L. CRICRÌ, voce *Videoregistrazioni*, in *Enc. giur.*, XXXII, Roma, 2006, p. 1.

[30] Ciascun *frame* rappresenta un dato digitale, espresso in codice binario, ossia una sequenza di numeri (0 e 1), i *bit*, i quali contengono le informazioni visive codificate e archiviate all'interno delle memorie digitali dei computer o di altri dispositivi informatici.

[31] Su questo punto si rimanda integralmente a W. NOCERINO, *Sulle modalità di acquisizione delle immagini provenienti dalle telecamere di videosorveglianza*, in *Cass. pen.*, 7-8, 2024, p. 2422.

[32] Ci si riferisce alla nota pronuncia delle sezioni unite "Prisco" che, da un lato, ha definito la natura documentale dei filmati acquisiti dalle telecamere di videosorveglianza effettuate da privati in luoghi pubblici, aperti o esposti al pubblico; dall'altra, ha chiarito che le videoriprese esperite dalla polizia giudiziaria a fini investigativi rientrano nella categoria delle prove atipiche (Cass. pen., S.U., 28 marzo 2006, n. 26795 in *CED Cass.*, n. 234270). Sulla pronuncia in esame, *ex multis*, A. CAMON, *Le Sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi*, in *Riv. it. dir. e proc. pen.*, 2006, p. 1550; C. CONTI,

Sezioni Unite riconduce le video riprese al regime delle intercettazioni solo limitatamente ai contributi di natura comunicativa, ricorrendo alla categoria della prova atipica per la documentazione di condotte non comunicative [33].

Al di là delle classificazioni operate per le video registrazioni su cui si tornerà più avanti [34], l'immagine estrapolata, se considerata autonomamente rispetto alla ripresa da cui proviene, è inquadrata come un documento informatico, in quanto rappresentazione di un fatto, di un dato o di un'informazione incorporata su un supporto digitale [35], oppure, di un atto tipico del procedimento [36], a seconda che il materiale sia stato prodotto fuori, ovvero nel corso del procedimento [37].

Le video-riprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi "riservati", in *Dir. pen. e proc.*, 2006, p. 1347; L. BELVINI, *Videoriprese non investigative e tutela della riservatezza*, in *Proc. pen. giust.*, 4, 2018, p. 797; N. TRIGGIANI, *Le videoriprese investigative e l'uso dei droni*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2019, p. 61; L. SAPONARO, *L'impatto processuale delle immagini: fotografie e videoriprese*, Wolters Kluwer Cedam, Padova, 2021; C. RIZZO, *Videoriprese in luoghi pubblici e poteri degli organi di polizia*, in *Cass. pen.*, 11/2024, p. 3584.

[33] Per un approfondimento sulla giurisprudenza successiva, cfr. N. TRIGGIANI, *Le videoriprese investigative tra Corte costituzionale e sezioni unite cronaca di una travagliata evoluzione giurisprudenziale (... in attesa del legislatore)*, in *Iurisdictio*, 4, 2023, p. 40-63.

[34] Cfr. *infra*, il § 5.

[35] Art. 234 c.p.p., cfr. sul punto W. NOCERINO, *Sulle modalità di acquisizione delle immagini provenienti dalle telecamere di videosorveglianza*, in *Cass. pen.*, 7-8, 2024, p. 2422.

[36] Secondo W. NOCERINO, *Sulle modalità di acquisizione delle immagini provenienti dalle telecamere di videosorveglianza*, cit., in questo caso, l'attività può ricadere entro la categoria degli «accertamenti urgenti, secondo il dettato dell'art. 354, comma 2, c.p.p., qualora il rilievo irripetibile sia eseguito dalla p.g. in situazioni "urgenti" in sede di "sopralluogo"; assicurazione delle fonti di prova, ai sensi dell'art. 348 c.p.p., nel caso in cui l'esigenza investigativa di acquisire le immagini emerga in un momento successivo all'"intervento" (*rectius*: assunzione della direzione dell'attività di indagine) del p.m.».

[37] In questo senso, P. TONINI, *L'evoluzione delle categorie tradizionali: il documento informatico*, in A. MANNA-A. CADOPPI-S. CANESTRARI-M. PAPA, *Cybercrime*, Utet, Torino, 2023, p. 1506. Più in generale, sull'inquadramento giuridico della categoria della prova documentale, *ex multis*, I. CALAMANDREI, *La prova documentale*, Cedam, 1995; L. KALB, *Il documento nel sistema probatorio*, Giappichelli, Torino, 2000; F. ZACCHÉ, *La prova documentale*, Giuffè, Milano, 2012.

3. *La rappresentazione digitalizzata del volto entro il* genus *della "prova digitale"*

L'unico comune denominatore tra i dati precedentemente esaminati sembra essere costituito dal tipo di supporto necessario per l'esecuzione di comparazioni tramite i sistemi automatizzati di riconoscimento facciale. Per poter garantire l'efficacia operativa e sfruttare la rapidità di questi strumenti, infatti, risulta imprescindibile la preliminare digitalizzazione della morfologia del volto, attraverso procedimenti di acquisizione e codifica che ne consentano una rappresentazione strutturata in formato digitale. Tale procedura costituisce il principale presupposto tecnico per il ricorso agli strumenti basati su modelli di analisi biometrica, i quali operano mediante l'estrazione di parametri distintivi e il confronto con i dati registrati.

La categoria giuridica in cui ricondurre le varie rappresentazioni digitalizzate del volto è quella della "prova digitale", intesa come «qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire a un sistema computerizzato di svolgere una funzione»[38].

Ai fini della presente analisi, però, è bene tenere presente che non è

[38] Art. 1, lett. b), della Convenzione di Budapest. Per un'analisi delle diverse definizioni cfr. G. ZICCARDI, *Scienze forensi e tecnologie informatiche*, in L. LUPARIA-G. ZICCARDI (a cura di), *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007, p. 3 ss. Giova ricordare altresì una suggestiva definizione di L. CUOMO, *La prova digitale*, in G. CANZIO-L. LUPARIA (a cura di), *Prova scientifica e processo penale*, Wolters Kluwer Cedam, Milano, 2017, p. 673, il quale afferma che «le prove digitali, costituite da *record*, file, codici sorgente, tracce digitali, programmi informatici e flussi di *bit*, per la loro natura immateriale variamente rappresentabile, sono raccolte in un luogo virtuale dove perde consistenza la naturale propensione dell'uomo a rapportarsi con il mondo circostante con l'uso dei sensi e, in particolare, con il tatto». Cfr. anche M. PITTIRUTI, *Digital evidence e procedimento penale*, Giappichelli, Torino, 2017, p. 8 e G. COSTABILE, *Digital forensics & digital investigation: classificazione, tecniche e line guida nazionali e internazionali*, in S. ATERNO-F. CAJANI-G. COSTABILE-D. CURTOTTI (a cura di), *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Giappichelli, Torino, 2021, p. 5, in cui si distingue fra "evidenze digitali" ed "evidenze non digitali": le prime sono «quelle fonti di prova memorizzate in strumenti informatici, come le postazioni di lavoro degli utenti, i *server* aziendali, il *cloud* o altri sistemi cd. informatici. Questo tipo di evidenze sono caratterizzate da una "carenza di fisicità" che porta ad una maggiore facilità di modifica accidentale durante la fase di acquisizione delle stesse», mentre le seconde sono definite come «quelle fonti di prova che non sono memorizzate in dispositivi informatici come, ad esempio, la stampa di un bollettino falso, del denaro contraffatto, ecc.».

necessario approfondire ogni aspetto relativo al trattamento della prova digitale [39]. È sufficiente qui esaminare l'inquadramento giuridico e tecnico della rappresentazione digitalizzata del volto per comprendere i diversi livelli di complessità che caratterizzano il risultato di un *match* biometrico automatico, sul quale invece ci si concentrerà specificamente per tentare un suo inquadramento. Si è già fatto cenno alla scarsa distintività, derivante dalla limitata unicità delle caratteristiche facciali rispetto ad altri dati biometrici più "individualizzanti", cui si associa la bassa permanenza, ovvero la tendenza del volto a subire modificazioni nel tempo a causa di fattori fisiologici o ambientali. A queste caratteristiche, come già in precedenza illustrato, si aggiunge l'ipervariabilità, che riflette la suscettibilità del dato a variazioni determinate da condizioni di acquisizione non uniformi [40].

Ulteriori elementi di complessità derivano poi proprio dalla natura digitale del supporto in cui è contenuta l'immagine impiegata per le comparazioni, nonché dalla possibilità che il dato biometrico sia stato *trasformato/convertito, ricavato* o *generato automaticamente* mediante procedimenti di elaborazione algoritmica prima di essere sottoposto all'eventuale estrazione dei *punti di repere* e poi a confronto con altri dati [41].

Venendo ora al *genus* di riferimento, si rivela particolarmente utile richiamare la nozione giuridica di *digital evidence*, introdotta in ambito sovranazionale dalla Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001 (Convenzione di Budapest), recepita nell'ordinamento italiano mediante la legge di autorizzazione alla ratifica n. 48/2008 e che qui si tenta di declinare con specifico riguardo alle prove biometriche in esame [42]. Come

---

[39] Lo studio di questo settore è affidato alla *computer forensics* che si occupa della preservazione, dell'identificazione, dell'acquisizione, della conservazione e della documentazione dei contenuti degli elaboratori elettronici o dei sistemi informativi in generale, allo scopo di evidenziare prove a fini di indagine. L. CUOMO, *La prova digitale*, in G. CANZIO-L. LUPARIA (a cura di), *Prova scientifica e processo penale*, Wolters Kluwer Cedam, Milano, 2017, p. 674. Cfr. anche A. TESTAGUZZA, *Digital forensics. Informatica giuridica e processo penale*, Wolters Kluwer Cedam, Milano, 2015, p. 10.

[40] Cfr. il capitolo II, § 4.6.

[41] Cfr. il capitolo II, § 4.

[42] CONSIGLIO D'EUROPA, *Convenzione sulla criminalità informatica*, Budapest, 23 novembre 2001. In particolare, la seconda sezione del testo, dedicata al diritto processuale, sancisce l'obbligo per gli Stati aderenti di adeguare il proprio diritto nazionale interno, al fine di assicurare la presenza di strumenti investigativi efficaci per l'accertamento dei fatti che coinvolgono elementi di prova digitali. Attraverso una serie di interventi normativi sulle disposizioni processuali nazionali, la trasposizione della Convenzione di Budapest ha comportato

è noto, il cardine dell'architettura normativa delineata è rappresentato dal concetto di "prova digitale", la cui ammissibilità risulta strettamente correlata alla definizione di specifiche modalità operative per la sua acquisizione e gestione. In tal senso, la sua affidabilità non può prescindere dal rispetto di procedure rigorose di raccolta, conservazione e analisi degli elementi probatori, le quali devono garantire integrità, autenticità e riproducibilità del dato.

La normativa raccomanda la necessità di trattare tutti i dati digitali in conformità alle cautele poste dalle *best practices* che prescrivono l'adozione di metodologie rigorose, finalizzate a preservare l'integrità e l'affidabilità dell'evidenza digitale, nonché a garantirne la tracciabilità e la verificabilità in ambito processuale [43]. Sotto il profilo tecnico-operativo, per assicurare la

---

l'inserimento nel tessuto codicistico di un'ampia gamma di strumenti investigativi specificamente finalizzati alla ricerca della prova digitale. In particolare, l'intervento ha riguardato in modo significativo l'ispezione e la perquisizione che impongono all'Autorità giudiziaria, in sede di ispezioni o perquisizioni di sistemi informatici o telematici, di adottare "*misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*". Il dettato dell'art. 254 *bis*, e gli artt. 254, 256, 260, 352 e 354 c.p.p. prescrivono, infatti, l'acquisizione di dati informatici "*mediante copia … su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità*". Per un approfondimento sul tema, cfr. D. LA MUSCATELLA, *Il trattamento della prova digitale nel sistema processuale penale italiano. Anamnesi e prognosi di una patologia classica, declinata in una (apparente) riforma*, in *Inf. e dir.*, anno XLI, XXIV, n. 1-2, 2015; L. MARAFIOTI, *Digital evidence e processo penale*, in *Cass. pen.*, 2011, p. 4509; G. VACIAGO, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli, Torino, 2012; V. COLAROCCO-T. GROTTO-G. VACIAGO, *La prova digitale. La casistica civile e penale e gli strumenti di acquisizione in ambito cloud*, Giuffrè, Milano, 2020; L. BARTOLI-G. LASAGNI, *Antifraud Investigations and Digital forensic: a Comparative Perspective*, in M. CAIANIELLO-A. CAMON (a cura di), *Digital Forensic Evidence. Towards Common European Standards in Antifraud Administrative and Criminal Investigations*, Wolters Kluwer Cedam, Milano, 2021; M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2, 2011, p. 284 ss.; F. RESTA, *La disciplina acquista maggiore organicità per rispondere alle esigenze applicative*, in *Guida dir.*, 16, 2008, p. 52; G. MARCOCCIO, *Convention on Cybercrime: novità per la conservazione dei dati*, in *www.interlex.it*; L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. e proc.*, 2008, p. 700.

[43] Sarebbe indispensabile che le autorità inquirenti si dotassero di *best practices* uniformi da osservare per la formazione della prova digitale. Diversamente, si rischia che la giurisprudenza possa riconoscere come prove digitali, documenti privi di autenticità. Per un approfondimento sul tema cfr. S. ATERNO, *Digital Forensics e scena criminis*, in D. CURTOTTI-L. SARAVO (a cura di), *Manuale delle investigazioni sulla scena del crimine*, Giappichelli, Torino, 2019, p. 782; G. COSTABILE, *Digital forensics & digital investigation: classificazione, tecniche e linee guida nazionali ed internazionali*, in S. ATERNO-F. CAJANI-G. COSTABILE-D. CURTOTTI (a cura di), *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*,

genuinità e l'integrità dei singoli fotogrammi digitalizzati, le linee guida impongono l'osservanza della cd. "catena di custodia" (*chain of custody*) [44]. Quest'ultima rappresenta l'insieme dei passaggi formali, tracciati manualmente o attraverso sistemi elettronici, mediante i quali il reperto (e le successive acquisizioni digitali) transita dalla fase di acquisizione sino ai successivi utilizzi nel procedimento penale.

Il rispetto dei protocolli è imprescindibile per prevenire alterazioni, manomissioni o contaminazioni del dato, garantendo così la continuità probatoria e la legittima utilizzabilità dell'evidenza digitale in sede processuale. Ogni operazione deve essere eseguita esclusivamente su una copia forense del file (cd. *copia-clone*), preservando l'originale inalterato, così da assicurare la possibilità di future verifiche indipendenti. L'attività di copia consiste nella realizzazione di un'immagine *bit* a *bit* del contenuto del supporto che consente poi di operare la successiva analisi forense su un *hard disk* [45].

Giappichelli, Torino, 2021, p. 20 ss.; R. BRIGHI-M. FERRAZZANO, *Digital forensics: best practices and perspectives*, in M. CAIANIELLO-A. CAMON (a cura di), *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations*, cit., p. 15-16 e G. CARIA, *Le quattro fasi dell'analisi forense: identificazione, acquisizione, analisi*, in M. IASELLI (a cura di), *Investigazioni digitali*, Giuffrè, Milano, 2020, p. 6; G. PAOLOZZI, *Relazione introduttiva*, in L. LUPARIA-L. MARAFIOTI-G. PAOLOZZI (a cura di), *Dimensione tecnologica e prova penale*, Giappichelli, Torino, 2019, p. 3.

[44] Si parla di "*chain of custody*" (letteralmente "catena di custodia") per intendere una serie di operazioni che garantiscono la genuinità della prova. Per un approfondimento cfr. M. DANIELE, *La prova digitale nel processo penale*, cit., p. 293; R. BRIGHI-M. FERRAZZANO, *Digital forensics: best practices and perspectives*, in M. CAIANIELLO-A. CAMON (a cura di), *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations*, cit., p. 15-16; G. CARIA, *Le quattro fasi dell'analisi forense: identificazione, acquisizione, analisi*, in M. IASELLI (a cura di), *Investigazioni digitali*, Giuffrè, Milano, 2020, p. 6; G. PAOLOZZI, *Relazione introduttiva*, in L. LUPARIA-L. MARAFIOTI-G. PAOLOZZI (a cura di), *Dimensione tecnologica e prova penale*, Giappichelli, Torino, 2019, p. 3. Alcuni Autori sostengono che, alla luce delle peculiari caratteristiche della prova biometrica, sarebbe opportuno sviluppare una catena di custodia biometrica (*biometric chain of custody*) specificamente calibrata sulle caratteristiche intrinseche del dato biometrico oggetto di analisi. Tale esigenza deriva dalla natura altamente sensibile e individualizzante di queste informazioni, nonché dalla loro suscettibilità a distorsioni, alterazioni o errori di elaborazione algoritmica, che potrebbero compromettere l'attendibilità del processo di acquisizione, conservazione e utilizzo a fini investigativi e probatori. In questo senso cfr. N. BARTLOW, *Establishing the digital chain of evidence in biometric systems*, West Virginia University, 2009, M. JACQUET-C. CHAMPOD, *Automated face recognition in forensic science: Review and perspectives*, in *Forensic Science International*, 307, 2020.

[45] Entro tale fase si è soliti distinguere le tracce digitali in due categorie: le "evidenze

Proprio in ragione della delicatezza di questa fase, il precedente momento di *individuazione* e *acquisizione* dovrebbe essere accuratamente documentato, al fine di garantire l'autenticità lungo l'intero ciclo di custodia. Quest'ultimo riveste particolare importanza per quei dati biometrici digitalizzati che, non essendo il risultato di un procedimento di digitalizzazione a partire da un campione grezzo [46], registrano e conservano un tratto biometrico [47]. Per esempio, ogni volta che s'intenda trattare filmati di videosorveglianza al fine di estrapolare un determinato *frame* per eseguire confronti fisionomici dei volti, sarà sempre necessario procedere sulla copia forense. In questi casi, fondamentale è la creazione della cd. impronta *hash* [48], un'immagine digitalizzata identica all'originale. Il programma che crea la copia non fa altro che scandire sequenzialmente uno dopo l'altro tutti i *byte* che costituiscono il file e ricavare, passo dopo passo, una serie di "impronte intermedie", ciascuna delle quali dipende dalla precedente, ottenendo, al termine della scansione, l'impronta *hash* definitiva. Ogni fase dell'elaborazione è influenzata da quelle precedenti, determinando lo stato di quelle successive e, per questo motivo, è sufficiente modificare anche un solo *bit* di tutto il file per ottenere un'impronta *hash* diversa. A tal proposito, in dottrina, è stato osservato come, nella fase delle indagini preliminari, i dati di natura digitale si caratterizzino per una strutturale dematerializzazione, nonché per una intrinseca fragilità e alterabilità, tali da incidere sensibilmente sulla loro stabilità e persistenza nel tempo [49]. Tali proprietà ontologiche del dato informatico comportano conseguenze rilevanti in termini di qualificazione

informatiche" (file testuali, multimediali o di archivio) la cui sola presenza può dare riscontro all'evento e alla condotta di un illecito, e i "programmi", ossia file che necessitano di un'analisi per divenire evidenti. Nel primo caso la data, l'ora, l'utente che ha creato il file, la sua eventuale cancellazione o modificazione possono essere informazioni utili per la ricostruzione del fatto e una corretta attribuzione della responsabilità in capo all'autore del fatto di reato.

[46] Cfr. il capitolo II, § 5.

[47] Ci si riferisce appunto alla categoria dei *dati generati automaticamente.*

[48] «(…) l'*hash* è una funzione non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita (…). È come un'impronta digitale per un file e deriva direttamente dal contenuto dell'oggetto da cui è stata generata». G. CARIA, *Le quattro fasi dell'analisi forense: identificazione, acquisizione, analisi*, cit., p. 15. Cfr. anche G. FAGGIOLI-A. GHIRARDINI, *Computer Forensics*, Apogeo, Milano, 2009, p. 71-73.

[49] Per un approfondimento cfr. P. TONINI, *Manuale di procedura penale*, Giuffrè, Milano, 2020, p. 358; M. TORRE, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale. La prova informatica nella legge 18 marzo 2008*, n. 48, in *Inf. dir.*, anno XLI, XXIV, n. 1-2, 2015, p. 71.

procedurale delle operazioni di acquisizione e analisi degli stessi. In particolare, queste peculiarità tecniche hanno indotto a ritenere applicabile alle attività di natura informatica il regime delle attività tecniche non ripetibili di cui all'art. 360 c.p.p., al fine di preservare il diritto alla partecipazione della difesa e garantire il contraddittorio anticipato [50]. Secondo tale ricostruzione, ogni operazione che implichi il rischio di modificazione, cancellazione o degradazione dei dati digitali, e che incida sul contenuto informativo degli stessi, dovrebbe essere qualificata come irripetibile, con la conseguente necessità di un previo avviso alla persona sottoposta alle indagini e al suo difensore, a pena di inutilizzabilità dell'atto [51].

Venendo all'inquadramento più strettamente processuale, inizialmente, la prova digitale è stata ricondotta nell'area di applicazione dell'art. 189 c.p.p. [52]. D'altronde, secondo alcuni autori, la norma sarebbe stata introdotta proprio con la *ratio* di rispondere alle sfide imposte dal «continuo sviluppo tecnologico che estende le frontiere dell'investigazione» [53].

---

[50] Cfr. M. DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012, p. 442; F. GIUNCHEDI, *Gli accertamenti tecnici irripetibili*, Giappichelli, Torino, 2009, p. 61 ss.; P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. e proc.*, 2009, p. 405 ss.; L. LUPARIA, *La disciplina processuale e le garanzie difensive*, in L. LUPARIA-G. ZICCARDI (a cura di), *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Giuffrè, Milano, 2007, p. 154 ss.

[51] Per una ricostruzione, cfr. M. MATTIUCCI, *Le indagini sui reperti invisibili. High tech crime*, in D. CURTOTTI-L. SARAVO (a cura di), *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze*, Giappichelli, Torino, 2013, p. 712; S. ATERNO, *Digital forensics e scena criminis*, in D. CURTOTTI-L. SARAVO (a cura di), *Manuale delle investigazioni sulla scena del crimine*, Giappichelli, Torino, 2019, p. 794. Di contrario avviso la giurisprudenza che ha ritenuto che l'estrazione di dati archiviati in un supporto informatico, quale è la memoria di un telefono cellulare, non costituisce accertamento tecnico irripetibile, e ciò neppure dopo l'entrata in vigore della legge 18 marzo 2008, n. 48, che ha introdotto unicamente l'obbligo di adottare modalità acquisitive idonee a garantire la conformità dei dati informatici acquisiti a quelli originali, con la conseguenza che né la mancata adozione di tali modalità, né, a monte, la mancata interlocuzione delle parti al riguardo comportano l'inutilizzabilità dei risultati probatori acquisiti, ferma la necessità di valutare, in concreto, la sussistenza di eventuali alterazioni dei dati originali e la corrispondenza ad essi di quelli estratti, Cass. pen., sez. I, 10 giugno 2021, n. 38909, in *CED Cass.*, n. 282072; Cass. pen., sez. II, n. 29061, 1 luglio 2015, in *CED Cass.*, n. 264572; Cass. pen., sez. V, 16 novembre 2015, n. 11905, in *CED Cass.*, n. 266477.

[52] Cfr. P. GUALTIERI, *Prova informatica e diritto di difesa*, in *Dir. pen. e proc.*, 2008, p. 70.

[53] Cfr. *Relazione al progetto preliminare del codice di procedura penale*, in G. CONSO-V.

Tuttavia, nel corso del tempo, l'orientamento esegetico è mutato. Si è infatti progressivamente fatta strada la percezione secondo cui per dare accesso alla prova digitale fossero sufficienti istituti tradizionali quali, nel nostro caso, in particolare, la perizia, la consulenza tecnica o la prova documentale [54]. Infatti, l'interpretazione letterale dell'art. 234 c.p.p. risulta compatibile con qualsiasi rappresentazione di fatti, persone o cose a prescindere dal mezzo utilizzato [55]. L'ampia formulazione della norma ha dunque aperto la strada a una concezione della prova digitale come documento, svincolata dalla necessità di un inquadramento nell'ambito delle prove atipiche, che trova ulteriore riscontro nella normativa di settore (d.lgs. 82/2005, c.d. Codice dell'amministrazione digitale), ove si definisce il documento informatico come qualsiasi «rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti» [56].

Di conseguenza, l'utilizzo di dati digitali nel processo penale è stato gradualmente "normalizzato" all'interno degli strumenti probatori tradizionali, pur con la necessità di verificare la loro affidabilità, integrità e pertinenza ai fini della decisione giudiziaria. L'impiego di modelli di intelligenza artificiale per l'estrazione o la generazione di dati utilizzati in ambito probatorio aggiunge un ulteriore livello di complessità e accentua i dubbi circa il corretto inquadramento processuale di tali risultati, ponendo interrogativi in merito

---

GREVI-G. NEPPI, *Il nuovo codice di procedura penale. Dalla legge delega ai decreti delegati*, vol. IV, *Il progetto preliminare del 1988*, Cedam, Padova, 1990, p. 553 ss. In dottrina, cfr. O. DOMINIONI, *La prova penale scientifica*, cit., p. 103 e 104. Di diversa opinione, cfr. G. UBERTIS, *Il giudice, la scienza e la prova*, in *Cass. pen.*, 11, 2011; F. CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processso penale*, in *Cass. pen.*, 9, 2008; V. BOZIO, *La prova atipica*, in P. FERRUA-E. MARZADURI-G. SPANGHER (a cura di), *La prova penale*, Utet, Torino, 2008, p. 66 ss.

[54] Rispettivamente artt. 233, 220 e 234 c.p.p. Cfr. Cass. pen., sez. III, 5 luglio 2012, n. 374119, in *CED Cass.*, n. 253573, Cass. pen., sez. VI, 20 dicembre 2018, n. 15838, in *CED Cass.*, n. 275541 e Cass. pen., sez. VI, 6 febbraio 2020, n. 12975, in *CED Cass.*, n. 278808. Cfr. M. PITTIRUTI, *Digital evidence*, cit., p. 20 e 23 ss.

[55] Cfr. L. KALB, *Il documento nel sistema probatorio*, Giappichelli, Torino, 2000, p. 72; D. La MUSCATELLA, *Il trattamento della prova digitale nel sistema processuale penale italiano. Anamnesi e prognosi di una patologia classica, declinata in una (apparente) riforma*, cit., p. 272; S. CONTI, *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Inf. e dir.*, anno XLI, XXIV, n. 1-2, 2015, p. 162; G. VACIAGO, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli, Torino, 2012, p. 1 ss.; S. MASON, *Electronic Evidence: Disclosure, Discovery and Admissibility*, LexisNexis, Londra, 2007, p. 22.

[56] Art. 1, comma 1, lett. p).

alla trasparenza del processo algoritmico[57], alla possibilità di comprensione e controllo delle operazioni svolte dal sistema, nonché all'eventuale e sempre possibile margine di errore e di *bias* nel funzionamento delle architetture di *machine learning*[58].

In tal senso, il successivo e diverso *match* biometrico, inteso come *output* di un confronto dinamico fra rappresentazioni di volti digitalizzati, non sembra già di per sé idoneo a essere collocato rigidamente all'interno delle tradizionali categorie probatorie del codice di rito, rifiutando generalizzazioni aprioristiche. La sua flessibilità ontologica e la varietà dei metodi con cui può essere trattato e analizzato impongono un approccio caso per caso, volto a individuare il regime giuridico più adeguato. In questo senso, la percentuale di compatibilità biometrica non si presta a un'univoca qualificazione giuridica, poiché essa dipende tanto dalla finalità procedimentale per cui il dato biometrico viene acquisito, elaborato e utilizzato, quanto dalla modalità operativa impiegata.

Ne discende la necessità di procedere ad una differenziazione degli scenari operativi in cui tale risultato di compatibilità viene generato e utilizzato, al fine di elaborare un quadro sistematico che, tenendo conto della *ratio* dell'acquisizione e delle peculiarità della modalità applicativa adottata, consenta di delineare la qualificazione giuridica più appropriata.

4. *La modalità applicativa* a posteriori*: nuovo trattamento o nuovo metodo?*

Una volta estratta la rappresentazione digitalizzata del dato, ovvero il suo modello elettronico e individuato uno o più volti "normalizzati", si può procedere con la fase di comparazione, alla ricerca di un *match.* Come visto[59], il sistema può operare *a posteriori.*

---

[57] Cfr. il capitolo III, § 4.1.

[58] G. CANZIO, *Intelligenza artificiale e processo penale*, in *Cass. pen.*, 3, 1 marzo 2021, p. 797; G. CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, in *Sist. pen.*, 8 gennaio 2021; S. QUATTROCOLO, *Prova e intelligenza artificiale*, in C. CONTI-A. MARANDOLA, *La prova scientifica*, cit., p. 477; S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, cit., 2020, p. 89 ss.

[59] Cfr. il capitolo II, § 4.

Se il dato biometrico grezzo, una volta digitalizzato, è suscettibile di diverse qualificazioni e inquadramenti a seconda del contesto applicativo in cui viene impiegato, la medesima considerazione – *mutatis mutandis* – può essere astrattamente estesa al *match* biometrico. Come si è già visto, anche il Garante privacy, nell'individuare il fondamento giuridico per l'utilizzo di SARI, nella modalità *a posteriori*, ha richiamato una serie di disposizioni normative elencate nella valutazione d'impatto dello strumento, riconducendone l'impiego a diverse attività processuali già codificate [60].

Laddove la comparazione fosse eseguita per finalità di stretta identificazione a procedimento penale già avviato, l'impiego dello strumento rientrerebbe tra le prerogative investigative della polizia giudiziaria, in conformità a quanto previsto dall'art. 349 comma 2 c.p.p. La norma segue una linea progressiva: dall'invito rivolto dalla polizia giudiziaria all'interessato a riferire le proprie generalità ed ogni altra notizia che possa essere utile ai fini identificativi, alla possibilità di eseguire – ove occorra [61] – rilievi dattiloscopici, fotografici e antropometrici [62], nonché «*altri accertamenti*» (comma 2) [63]. L'espressione designa un insieme di operazioni variegate che la polizia giudiziaria può eseguire nell'ambito delle attività di identificazione della persona sottoposta a indagini, qualora le modalità ordinarie non risultino idonee al raggiungimento dello scopo. La disposizione sembra riferirsi a operazioni strumentali che non assumono natura invasiva [64], come la comparazione di dati fotografici o la raccolta di informazioni descrittive utili all'attribuzione dell'identità. Rimane imprescindibile il principio secondo cui le operazioni di accertamento meramente identificativo non possono in alcun modo sconfinare in attività riconducibili alla fase istruttoria, né essere

[60] Cfr. capitolo IV, § 2.

[61] L'inciso consente il compimento dei suddetti accertamenti solo in via sussidiaria, allorché non si sia riusciti ad ottenere l'identificazione mediante la modalità di cui al primo comma, ovvero quando la persona si sia rifiutata di fornire le proprie generalità o siano sorti dubbi in merito a queste.

[62] L'attività consiste nella misurazione di determinate parti del corpo (a titolo esemplificativo, si ricorda la statura, la lunghezza del tronco, l'apertura delle braccia): tutti questi dati (non annoverabili fra quelli "biometrici") vengono, poi, classificati in gruppi entro i quali si individua il soggetto da identificare.

[63] Si tratta di una locuzione di chiusura della norma che lascia aperto il catalogo delle nuove tecnologie che l'evoluzione scientifica può fornire.

[64] Cfr. *ex multis* Cass. pen., sez. IV, 29 marzo 2017, n. 19044, in *Guida dir.*, 23, 83, 2017; Cass. pen., 31 gennaio 2017, n. 11082, in *CED Cass.*, n. 2017.

funzionali alla formazione del compendio probatorio. Tale distinzione, d'altronde, è imposta da un'esigenza di tutela strutturale del diritto di difesa, il cui presidio si esplica in un sistema di garanzie processuali specificamente previste per gli atti di investigazione e per l'acquisizione di prove in senso stretto.

Nel caso in cui la condotta dell'autorità procedente si traduca, in concreto, in un'attività finalizzata non più soltanto all'identificazione della persona, ma all'acquisizione di informazioni incidenti sulla ricostruzione dei fatti oggetto del procedimento, si determinerebbe una *mutatio naturae* dell'atto, che richiederebbe l'attivazione delle forme di garanzia previste per gli atti di indagine irripetibili o per quelli eseguiti coattivamente. L'omessa attivazione di tali garanzie – si pensi, ad esempio, alla mancata presenza del difensore o alla mancata autorizzazione del giudice – comporta un vizio genetico dell'atto, tale da inficiare, talvolta, l'utilizzabilità del dato acquisito.

Da queste attività va tenuta distinta l'identificazione compiuta dalla polizia per finalità di sicurezza, svolta nel corso di operazioni preventive, a tutela della collettività, che gode di un'autonoma disciplina. Ai sensi dell'art. 11, d.l. 21 marzo 1978, n. 5, convertito con modificazioni dalla legge 18 maggio 1978, n. 191, l'identificazione viene compiuta dagli ufficiali e dagli agenti di polizia nei confronti di chi rifiuta di dichiarare le proprie generalità, oppure rende dichiarazioni o esibisce documenti in relazione ai quali ricorrono sufficienti indizi per ritenerne la falsità. Inoltre, l'art. 4 TULPS [65] stabilisce che, nei confronti di determinate persone pericolose o sospette, oppure cittadini stranieri, che non sono in grado o si rifiutano di provare la propria identità, l'autorità di pubblica sicurezza è obbligata, per gli stranieri – mentre ha facoltà, per gli altri – ad eseguire «*rilievi segnaletici*». La formulazione generica della norma apre la possibilità di estendere l'ambito applicativo delle tecnologie di riconoscimento facciale automatizzato, anche al di fuori di contesti strettamente processuali, legittimandone l'impiego in operazioni di polizia preventiva e di sicurezza pubblica [66]. La norma, nel lasciare ampio margine di discrezionalità operativa all'autorità, non fornisce indicazioni specifiche in merito alla natura e alla tipologia dei dati che possono essere acquisiti, né

[65] R.d. 18 giugno 1931, n. 773.

[66] Cfr. I. NERONI REZENDE, *Facial Recognition for Preventive Purposes: The Human Rights Implications of Detecting Emotions in Public Spaces*, in L. BACHMAIER WINTER-S. RUGGERI (a cura di), *Investigating and Preventing Crime in the Digital Era. Legal Studies in International, European and Comparative Criminal Law*, vol 7, Springer, Cham, 2022; V.L. RAPOSO-L. DU, *Facial recognition technology: is it ready to be used in public health surveillance?*, in *Int. Data Privacy Law*, Vol. 14, Issue 1, 2024, p. 66-86.

stabilisce limiti procedurali stringenti sull'impiego di strumenti tecnologici avanzati, come i sistemi di riconoscimento facciale basati su intelligenza artificiale. Proprio questa genericità del dettato normativo, che riflette l'arretratezza del testo rispetto alle più recenti evoluzioni tecnologiche, è stata interpretata dal Garante come base giuridica sufficiente per giustificare, *de facto*, l'utilizzo di sistemi automatizzati di riconoscimento facciale anche in contesti non rigidamente connessi a un procedimento penale, ma funzionali al mantenimento dell'ordine pubblico e alla prevenzione dei reati.

In linea teorica, l'attività di comparazione eseguita *a posteriori*, poi, potrebbe anche essere inquadrata tra gli atti compiuti di propria iniziativa dalla polizia giudiziaria o su delega del pubblico ministero e volti all'assicurazione delle fonti di prova, ai sensi del combinato disposto degli artt. 55 e 348 c.p.p., ovvero tra gli accertamenti e i rilievi sulle persone, diversi dalle ispezioni personali, che possono essere eseguiti dagli ufficiali di polizia giudiziaria in situazioni di necessità [67]. Si tratta, in tal caso, di operazioni funzionali alla preliminare assicurazione delle fonti di prova, da intendersi come strumenti di cognizione prodromici al successivo accertamento giudiziale, purché non siano connotati da una particolare invasività nella sfera giuridica individuale e siano eseguiti nel rispetto delle garanzie procedurali minime previste dall'ordinamento [68]. All'attività autonoma della polizia giudiziaria, si somma quella del pubblico ministero che abbia già assunto la direzione delle indagini: qualora si renda necessario procedere a confronti automatizzati mediante un sistema di riconoscimento facciale *a posteriori* e l'attività di trattamento della rappresentazione digitalizzata del volto o l'operazione di comparazione tra dati biometrici presenti un elevato grado di complessità tecnica, tale da richiedere particolari competenze specialistiche, posta la ripetibilità della comparazione automatizzata fra volti, l'attività in questione potrebbe anche eventualmente rientrare nell'ambito applicativo degli accertamenti disciplinati dall'art. 359 c.p.p. [69]. In questa prospettiva, la comparazione

---

[67] Cfr. T. ALESCI, *Il corpo umano come fonte di prova*, cit., p. 71. Per un'analisi in termini giuridico-processuali dell'attività investigativa che ordinariamente viene compiuta sulla scena del crimine dalla polizia giudiziaria, si v. A. CHELO, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, Wolters Kluwer Cedam, Milano, 2014.

[68] Per un approfondimento, cfr. R. D'ALESSIO, *Sub art. 348*, in *Codice di procedura penale. Rassegna di giurisprudenza e dottrina*, G. LATTANZI-E. LUPO (a cura di), Giuffrè, Milano, 2017.

[69] Cfr. A. MARI, *Sub art. 359*, in *Codice di procedura penale. Rassegna di giurisprudenza e dottrina*, G. LATTANZI-E. LUPO (a cura di), vol. V, Giuffrè, Milano, 2017.

biometrica non si configurerebbe come un mero "rilievo" descrittivo, bensì, implicando un procedimento analitico strutturato che impiega modelli computazionali avanzati per l'elaborazione dei tratti biometrici, potrebbe essere fatto ragionevolmente rientrare nella categoria degli "accertamenti". L'*iter* del riconoscimento automatizzato, caratterizzato dall'applicazione di metodologie tecnico-scientifiche e di sistemi basati su intelligenza artificiale e *machine learning*, consente di qualificare l'attività di riconoscimento facciale *a posteriori* come un accertamento ripetibile, distinto dai rilievi in ragione della sua natura valutativa [70].

Oltre a queste operazioni, il sistema di riconoscimento facciale *a posteriori* parrebbe astrattamente idoneo a svolgere anche ulteriori funzioni riconducibili al *genus* dell'individuazione disciplinata dall'art. 361 c.p.p. [71], o della ricognizione di persone, regolata dagli artt. 213 e ss. c.p.p., a seconda che l'atto abbia rispettivamente una funzione investigativa o probatoria [72]. In entrambe le ipotesi considerate, ci si trova dinanzi ad un'attività atipica [73], in quanto il soggetto preposto al riconoscimento non è un individuo, ma un sistema automatizzato. Nondimeno, l'atipicità del mezzo di prova o del mezzo di ricerca della prova non rappresenta ovviamente di per sé un

---

[70] Cfr. S. LORUSSO, *L'esame della scena del crimine nella contesa processuale*, in *Dir. pen. e proc.*, 2011, p. 264 e A. SCALFATI, *Gli accertamenti tecnici dell'accusa*, in *Ind. pen.*, 1992, p. 130.

[71] In una sentenza della Corte di Cassazione del 2020 si sono potuti dedurre altri possibili utilizzi oltre all'identificazione. Un pubblico ministero di Milano ha utilizzato SARI per analizzare il volto di una persona coinvolta in una rissa con altri quattro soggetti, confrontando le immagini registrate da un sistema di videosorveglianza con i volti «presenti su utenze telefoniche» (verosimilmente si tratta delle foto profilo di Whatsapp). Il p.m. ha utilizzato questo risultato a supporto della richiesta di applicazione di una misura cautelare. Cass. pen., sez. I, 21 luglio 2020, n. 21823, *inedita.*

[72] Cfr. A. MARANDOLA, *Il riconoscimento facciale*, in C. CONTI-A. MARANDOLA, *La prova scientifica*, Giuffrè, Milano, 2023, p. 500 ss.; M. TORRE, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. e proc.*, 8, 2021; R. LOPEZ, *La rappresentazione facciale tramite software*, in A SCALFATI (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2019, p. 311 ss.; volendo, E. SACCHETTO, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *Leg. pen.*, 16 ottobre 2020.

[73] «Nel sistema attuale l'atipicità consiste […] nell'utilizzare componenti non tipiche all'interno di un mezzo tipico». Così, P. TONINI, *Manuale di procedura penale*, XXV ed., 2024, p. 305. Per un approfondimento, cfr. A. MELCHIONDA, voce *Prova in generale (dir. proc. pen.)*, in *Enc. dir.*, *Agg.*, I, Milano, 1997, p. 838; A. PROCACCINO, *Prove atipiche*, in A. GAITO (a cura di), *La prova penale*, I, Utet, Torino, 2009, 268; P. TONINI, C. CONTI, *Il diritto delle prove penali*, Giuffrè, Milano, 2014.

elemento ostativo alla sua ammissione, purché però lo strumento tecnologico impiegato soddisfi determinati requisiti e non eluda le garanzie previste per il relativo strumento tipico [74].

4.1. *Il riconoscimento a posteriori e la categoria della prova atipica*

Come noto, ai sensi dell'art. 189 c.p.p., affinché una prova atipica possa concretamente ritenersi ammissibile, è necessario che essa risponda a due criteri fondamentali: l'*idoneità* ad assicurare l'accertamento dei fatti e il *rispetto della libertà morale* della persona coinvolta nel procedimento [75].

Il primo requisito attiene alla capacità dello strumento tecnologico di produrre risultati attendibili, verificabili e ripetibili. Quando si tratti di una prova scientifica l'idoneità è tradizionalmente valutata alla luce di specifici criteri metodologici, la cui osservanza è indispensabile affinché un risultato tecnico possa acquisire rilevanza probatoria nel contesto giuridico [76]. In

---

[74] Cfr. *infra* il § 6.

[75] A. MELCHIONDA, voce *Prova in generale (dir. proc. pen.)*, cit., p. 839 ss.

[76] C.d. criteri *Daubert*, dalla nota sentenza della Corte Suprema americana (1993) nel caso *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993). La pronuncia è giunta a definire gli elementi indispensabili della prova scientifica nel processo penale (*in primis* negli USA, poi diffusa e recepita da molti altri ordinamenti giuridici nazionali tra cui l'Italia). I punti cardine della sentenza sono: a) la verificabilità del metodo (una teoria è scientifica solo se controllabile mediante esperimenti); b) la falsificabilità (sottoporsi a tentativi di smentita ed individuare con certezza i limiti della stessa teoria); c) la conoscenza del tasso di errore (è necessario comunicare al giudice l'ipotesi di errore calcolata e consentire al giudice stesso il ruolo di *gatekeeper*, o meglio di "custode" della prova scientifica); d) la sottoposizione al controllo della comunità scientifica (consente un controllo capillare da parte degli esperti del settore tramite la pubblicazione delle tesi scientifiche nelle riviste specializzate). La successiva sentenza *Kumho Tire e Co. del 1999* ha esteso i criteri alla ammissione degli esperti in materie che richiedono specifiche conoscenze di tipo non scientifico (U.S. Supreme Court 23 marzo 1999, *Kumho Tire Co. c. Carmichael*). Questi standard sono stati poi espressamente regolamentati nella *Rule* 702 delle "*Federal Rules of Evidence*" (2011), come segue: 1) la prova peritale è il prodotto del metodo scientifico, empiricamente resistente alla prova contraria; 2) l'apporto metodologico deve esser revisionato da esperti diversi e pubblicato; 3) il margine di errore è necessariamente conoscibile; 4) la tecnica è costantemente monitorata, in termini di rispondenza a parametri standard; 5) la tecnica e il relativo apporto metodologico sono avallati dalla comunità scientifica. In Italia, il riferimento è a Cass. pen., S.U., 10 luglio 2002, n. 30328, Franzese, in *Cass. pen.*, 2002, p. 3643, nonché a Cass. pen., sez. IV, 17 settembre 2010, n. 43786, in *CED Cass.*, n. 248943. Per una ricostruzione approfondita si veda O. DOMINIONI, *La prova penale scientifica*, cit., p. 113 ss.; G. CARLIZZI, *La valutazione della prova*

particolare, la validità di una prova scientifica dipende dalla verificabilità del metodo impiegato, intesa come la possibilità di sottoporre il procedimento utilizzato a un esame critico volto a confermarne la correttezza e l'attendibilità. A ciò si aggiunge il vaglio sulla falsificabilità, ovvero la capacità del modello scientifico di essere sottoposto a confutazione attraverso esperimenti o analisi indipendenti, conformemente ai principi della metodologia scientifica di matrice popperiana [77].

Ulteriore parametro determinante è costituito dalla sottoposizione del metodo al controllo della comunità scientifica, il quale garantisce che la procedura adottata sia oggetto di un continuo scrutinio da parte degli esperti del settore, così da consolidarne la validità o metterne in discussione eventuali limiti e criticità. A ciò si affianca la necessità di una conoscenza del tasso di errore del sistema impiegato, elemento essenziale per valutare la precisione dei risultati ottenuti e per prevenire margini di indeterminatezza incompatibili con il principio di certezza del diritto.

Mettere in discussione l'*idoneità* di un sistema di riconoscimento facciale *a posteriori* a provare fatti di cui all'art. 187 c.p.p. solleva delle problematiche di non poco conto, tanto per la parte che introduce la prova, quanto per quella chiamata a confutarla. Infatti, essendo tale tecnologia caratterizzata da sostanziale opacità che incide direttamente sulla verificabilità e sulla riproducibilità dei risultati ottenuti [78] non è agevole né offrire la dimostrazione della idoneità, né contestare tale caratteristica. L'impiego di detti strumenti nell'ambito del processo penale solleva, dunque, delicati problemi in termini di accesso alla prova, conoscibilità del procedimento di formazione del dato e possibilità di esercitare, in modo effettivo e non meramente formale, il

---

scientifica, Giuffrè, Milano, p. 89 ss.; P. TONINI, *La Cassazione accoglie i criteri Daubert sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza*, in *Dir. pen. e proc.*, 11, 2011, p. 1341 ss.; M. BARGIS, *Note in tema di prova scientifica nel processo penale*, in *Riv. dir. proc.*, 2011, p. 51.

[77] Cfr. K. POPPER, *Logik der Forschung*, Wien, 1935, trad. it. M. TRINCHERO, *Logica della scoperta scientifica*, Einaudi, Torino, 1970, p. 22 e K. POPPER, *The poverty of the historicism* (1944-1945), trad. it. S. VECA, *Miseria dello storicismo*, Feltrinelli, Milano, 1997, p. 120: «la scoperta di esempi che convalidano una teoria vale pochissimo se non abbiamo tentato, senza riuscirvi, di trovare degli esempi che la confutano. Perché, se abbiamo poco senso critico, troveremo sempre quello che desideriamo: cercheremo e troveremo delle conferme; distoglieremo lo sguardo da ciò (e quindi non lo vedremo) che potrebbe mettere in pericolo le teorie che ci sono care. In questo modo è facilissimo ottenere prove apparentemente schiaccianti di una teoria che, se fosse stata invece avvicinata con animo critico, sarebbe confutata».

[78] Cfr. il capitolo III, § 5.

diritto al contraddittorio e, in ultima analisi, di fruire della imprescindibile parità delle armi, nella prospettiva già sopra illustrata [79].

In argomento, appare inevitabile un richiamo a una delle rare pronunce della giurisprudenza di legittimità che ha affrontato, seppur in via incidentale, il tema in esame [80]. Nel rigettare le doglianze difensive con le quali si contestava il mancato accoglimento da parte della Corte d'Appello della richiesta di rinnovazione dell'istruttoria dibattimentale, al fine di «procedere al riconoscimento facciale dell'imputato tramite la moderna tecnica SARI», i giudici hanno sottolineato come «la difesa non avesse in alcun modo documentato la valenza scientifica dell'anzidetta tecnologia». Tale affermazione, per quanto formalmente corretta sul piano processuale, appare problematica sotto un profilo sostanziale, poiché presuppone, in capo alla parte interessata, un onere probatorio che difficilmente può essere assolto. Infatti, l'impossibilità, o quantomeno l'estrema difficoltà di superare l'opacità che circonda l'idoneità probatoria del dato di cui si chiede l'ammissione, si traduce in una sostanziale menomazione del diritto alla prova e del principio di parità delle armi. Elemento paradigmatico di questa mancanza di trasparenza è rappresentato dall'origine dei dati impiegati per l'addestramento dell'algoritmo. La qualità, la provenienza e la rappresentatività del *dataset* di riferimento sono fattori determinanti per valutare l'affidabilità del sistema, poiché eventuali *bias* nei dati utilizzati per la fase di *training* possono tradursi in discriminazioni sistematiche o in errori di identificazione [81]. L'assenza di informazioni accessibili sulla composizione di tali *dataset* e, in generale, sul funzionamento degli strumenti impedisce di escludere il rischio che il modello algoritmico operi in modo distorto o selettivo, compromettendo così la neutralità e l'affidabilità dei risultati ottenuti.

La problematica appena descritta si accentua in maniera particolare a fronte dell'impiego, da parte degli investigatori, di software di riconoscimento facciale che si traduce in un *deficit* di verificabilità e, spesso, in una lesione al diritto di difesa, che non può dispiegarsi in modo pieno ed effettivo in assenza di un accesso trasparente ai criteri di formazione dell'*output*.

A conferma di tale criticità si evidenzia che, nonostante il SARI sia

---

[79] Cfr. il capitolo III, § 5.

[80] Cfr. Cass. pen., sez. IV, 18 giugno 2019, n. 39731, *inedita.* Si trova un cenno sulla pronuncia del 2019 anche in C. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato*, cit., p. 7. Un'ulteriore pronuncia ove si fa cenno a SARI è Cass. pen., sez. I, 21 luglio 2020, n. 21823, *inedita.*

[81] Cfr. il capitolo II, § 4.6.

operativo in Italia da circa sette anni, solo di recente e in seguito ad alcune sollecitazioni, sono state rese pubbliche informazioni ufficiali in merito all'incidenza percentuale delle comparazioni effettuate mediante tale tecnologia [82]. In particolare, «nell'anno 2022 si contano 79.362 ricerche, mentre nel 2023 sono state 131.023. Si registra quindi un aumento di oltre il 65%» [83].

Peraltro, non si dispone di dati certi relativi al tasso di falsi positivi e falsi negativi del sistema, il che impedisce di valutarne con rigore scientifico l'effettiva affidabilità e precisione nell'ambito delle operazioni di riconoscimento biometrico. L'assenza di trasparenza in relazione a tali parametri rappresenta un elemento di criticità, in quanto impedisce una valutazione empirica delle identificazioni effettuate [84].

Ulteriore elemento di indeterminatezza è costituito dalla mancata divulgazione di informazioni circa eventuali processi di affinamento e miglioramento dell'algoritmo da parte degli sviluppatori del sistema [85]. La continua

---

[82] Cfr. R. COLUCCINI-A. GIANNINI-L. SOTTILE, *Il Viminale ci tiene all'oscuro su come e quanto usa il sistema di riconoscimento facciale*, su https://irpimedia.irpi.eu/sorveglianze-viminale-riconoscimento-facciale-trasparenza/, 2024.

[83] Cfr. R. COLUCCINI-A. GIANNINI-L. SOTTILE, *Il Viminale ci tiene all'oscuro su come e quanto usa il sistema di riconoscimento facciale*, cit. Non è possibile determinare se l'incremento sia dovuto a un maggiore numero di operatori autorizzati all'uso del sistema o, piuttosto, a una maggiore frequenza di utilizzo da parte di un numero invariato di utenti. L'assenza di dati aggiornati sul numero di operatori abilitati a utilizzare SARI impedisce una valutazione chiara della sua diffusione operativa all'interno delle forze dell'ordine. L'unica fonte disponibile su tale aspetto è rintracciabile in una presentazione dell'azienda sviluppatrice del sistema Reco 3.26, dalla quale emerge che, fino a marzo 2019, erano state effettuate 121.743 ricerche da parte di 3.207 operatori. Tuttavia, ad oggi, non sono disponibili informazioni aggiornate sul numero effettivo di utenti autorizzati, né sull'attuale volume di utilizzo del sistema.

[84] Un utile termine di confronto è rappresentato dall'esperienza dei Paesi Bassi, dove sono stati pubblicati dati statistici relativi all'impiego di un sistema analogo da parte della polizia (*Catch*). In tale contesto, l'efficacia del riconoscimento facciale risulta limitata con una percentuale di corrispondenza compresa tra l'8% e il 12% dei casi. In Italia, un'analoga analisi quantitativa non è disponibile, in quanto le autorità competenti ritengono che tali informazioni costituiscano "risultati operativi" riferibili a specifiche indagini di polizia giudiziaria e, pertanto, non soggetti a divulgazione pubblica. Cfr. R. COLUCCINI-A. GIANNINI-L. SOTTILE, *Il Viminale ci tiene all'oscuro su come e quanto usa il sistema di riconoscimento facciale*, cit.

[85] Per quanto concerne l'accuratezza dell'algoritmo impiegato, gli unici dati pubblici disponibili risalgono al 2016. Ciò solleva dubbi circa l'aggiornamento e il miglioramento delle prestazioni del sistema nel tempo. Cfr. M. DEL COCO-P. CARCAGNÌ, *Face recognition*

evoluzione dei modelli di intelligenza artificiale e delle tecniche di *machine learning* impone un costante aggiornamento dei software, al fine di migliorarne le prestazioni, ridurre i margini di errore e garantire un utilizzo conforme ai criteri di scientificità richiesti per il loro impiego in ambito forense.

Pertanto, allo stato attuale, è davvero complesso verificare l'*idoneità* di questa modalità operativa per l'accertamento dei fatti, «in considerazione dei molti quesiti sollevati sul funzionamento del SARI, tuttora senza risposta, [dal momento che] la garanzia della sua affidabilità ricognitiva […] è flebile, in quanto esito di una procedura blindata e di dati ignoti» [86].

4.1.1. *Il requisito della libertà morale*

Il secondo requisito richiesto dall'art. 189 c.p.p. è finalizzato a garantire che il ricorso alla prova atipica non si traduca in una compressione indebita della *libertà morale* della persona che potrebbe risultare compromessa da pratiche invasive o sproporzionate [87]. Come visto, su questo aspetto non vi è unanimità di vedute [88]. Da un lato, si sostiene che la modalità operativa basata sull'elaborazione di immagini statiche non determini una compressione della libertà morale delle persone sottoposte a identificazione, individuazione o riconoscimento. In particolare, l'assenza di un'interazione diretta tra la persona e il sistema algoritmico, così come la natura mediata del trattamento (che si svolge, per l'appunto, sulla base di materiale preesistente), sottrarrebbe l'operazione ai rischi tipici delle forme di coercizione psichica [89].

Di tutt'altro avviso l'opinione che ritiene l'impiego della tecnologia di riconoscimento facciale – indipendentemente dal momento in cui viene eseguita la comparazione – portatore di effetti significativamente restrittivi sulle libertà individuali, compresa quella di autodeterminazione [90]. Secondo

---

algorithms: performance evaluation, su https://www.parsec326.it/images/doc/Report_Reco-Performance-Evaluation---CNR.PDF

[86] Così, R. LOPEZ, *La rappresentazione facciale tramite software*, cit., 257.

[87] P. TONINI-C. CONTI, *Il diritto delle prove penali*, cit., p. 196.

[88] Cfr. il capitolo III, § 2.

[89] Di questo avviso il provvedimento del Garante per la protezione dei dati personali sul Sistema automatico di ricerca dell'identità di un volto, 26 luglio 2018, n. 440, doc. web n. 9040256, in www.garanteprivacy.it. Cfr. il capitolo IV, § 2.

[90] Cfr. L. CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, in *Riv. it. dir. e proc. pen.*, 1, 1 marzo 2024, p. 233; F. PAOLUCCI, *From Global Standards to Local Safeguards: The AI Act, Biometrics, and Fundamental Rights*, in *SSRN*, 2024; F. RAGAZZI *et al.*, *Biometric*

questo opposto orientamento, l'impiego di tale strumento, ad esempio, subito dopo una manifestazione politica, al pari di una ripresa *in tempo reale*, potrebbe produrre un effetto dissuasivo rispetto all'esercizio della libertà personale, in quanto i soggetti coinvolti potrebbero percepire un rischio concreto di sorveglianza sistematica e di successiva identificazione, con possibili conseguenze giuridiche o sociali.

Permangono dunque significative difficoltà interpretative che, ad oggi, non hanno ancora trovato una soluzione univoca. Sebbene la modalità *enterprise* di SARI abbia positivamente superato il vaglio del Garante privacy, persistono numerosi interrogativi in merito alla sua ammissibilità processuale come mezzo di prova [91]. Ciò in ragione del fatto che essa non sembra in grado di rispettare unanimamente alcuno dei presupposti fissati dall'ordinamento affinché gli strumenti non disciplinati dalla legge possano essere impiegati legittimamente nel procedimento penale.

Ne discende, dunque, che, in assenza di un quadro normativo specifico che ne consenta l'impiego, regolamentandone casi, modalità e limiti e in attesa che le disposizioni contenute nel regolamento (UE) 2024/1689 siano implementate a livello nazionale, le individuazioni o le ricognizioni algoritmiche, effettuate mediante SARI *enterprise*, dovrebbero ritenersi precluse [92]. Seguendo l'interpretazione fornita dal Garante, però, non sembrerebbero emergere particolari elementi di criticità qualora l'impiego della modalità *a posteriori* fosse limitato al raggiungimento di finalità esclusivamente identificative durante le indagini, inquadrando l'attività tra gli «*altri accertamenti*» dell'art. 349, comma 2, c.p.p. [93]. Ne consegue che, in considerazione dell'assenza di adeguate garanzie, l'esito del *match* biometrico non dovrebbe in alcun caso trovare utilizzazione nelle successive fasi del procedimento.

& Behavioural Mass Surveillance in EU Member States: report for the Greens/EFA in the European Parliament. Brussels: Greens/EFA, 2021; EDPB-GEPD, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale)*, 18 giugno 2021, p. 13.

[91] Cfr. G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *Leg. pen.*, 11 dicembre 2021, p. 16 ss.; M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio,* in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Giuffrè, Milano, 2021, p. 64; M. TORRE, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. e proc.*, 8, 2021 p. 1053.

[92] Cfr. J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, cit., p. 178.

[93] Cfr. M. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., p. 64.

L'assenza di adeguati presidi relega dunque questo strumento a mero ausilio nell'ambito delle attività investigative di polizia giudiziaria. Laddove, invece, si perseguissero specifiche finalità probatorie, come più sopra evidenziato, la parte che intendesse ricorrere ad un consulente tecnico – in particolare, il pubblico ministero attraverso l'art. 359 c.p.p. e le difese *ex* artt. 233 e 327 *bis* c.p.p. – dovrebbe aver cura di incaricare l'esperto di illustrare anche, ove ciò sia possibile, le modalità di funzionamento e le caratteristiche dei software. Questi ultimi, infatti, anche alla luce dell'art. 13 del regolamento (UE) 2024/1689, dovranno essere «progettati e sviluppati in un modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire ai *deployers* di interpretare l'*output* del sistema e utilizzarlo adeguatamente».

5. *La modalità applicativa* in tempo reale

L'esame del quadro normativo interno ha già messo in luce l'inadeguatezza e la carenza sistematica della disciplina vigente in relazione alla regolamentazione dei sistemi di riconoscimento facciale operanti *in tempo reale* [94]. A livello europeo, il regolamento sull'intelligenza artificiale, pur rappresentando il primo riferimento normativo fondamentale per l'adozione di standard comuni, non costituisce di per sé la base giuridica per il trattamento dei dati biometrici, così come richiesto dall'art. 8 LED, limitandosi a fornire indicazioni di carattere generale ai legislatori nazionali, chiamati a definire e adottare una disciplina conforme ai principi delineati a livello europeo [95].

In vista dell'effettiva implementazione, a livello nazionale, di uno specifico *corpus* di norme che regolamenti il ricorso a questa particolare modalità applicativa, l'art. 382 *bis* c.p.p. sembra offrire un primo riferimento normativo suscettibile di essere valorizzato in sede interpretativa [96]. Tuttavia, per le

[94] Cfr. il capitolo IV.

[95] Cfr. considerando 38.

[96] Introdotto nel codice di rito dalla legge 24 novembre 2023, n. 168 e successivamente modificato dalla legge 18 novembre 2024, n. 171 recante «Misure urgenti per contrastare i fenomeni di violenza nei confronti dei professionisti sanitari, socio-sanitari, ausiliari e di assistenza e cura nell'esercizio delle loro funzioni nonché di danneggiamento dei beni destinati all'assistenza sanitaria», in *G.U.*, Serie Generale, n. 276 del 25 novembre 2024. L'istituto della

ragioni che si esporranno, permangono rilevanti riserve in merito alla riconducibilità strutturale del riconoscimento facciale *in tempo reale* al paradigma processuale delineato dalla norma. La disposizione, infatti, prevede la possibilità di procedere all'arresto anche oltre i limiti della flagranza, purché l'azione sia effettuata entro quarantotto ore dal fatto e sia fondata su una «documentazione video-fotografica o di altra documentazione legittimamente ottenuta da dispositivi di comunicazione informatica o telematica», idonea a ricostruire «inequivocabilmente» tanto gli elementi oggettivi della condotta, quanto l'identità del soggetto agente [97]. Tale riferimento alla "inequivocabilità" impone un'analisi particolarmente rigorosa del materiale documentale, richiedendo che esso presenti una capacità dimostrativa tale da non lasciare margini di incertezza sulla riferibilità soggettiva e sulle effettive modalità di commissione del reato. L'articolato normativo, pur non menzionando espressamente l'impiego di tecnologie biometriche o di sistemi automatizzati di riconoscimento facciale, può tuttavia essere interpretato come

---

flagranza differita è stato inserito nel nostro ordinamento dal d.l. n. 28/2003 con riferimento ai reati commessi con violenza alle persone o alle cose in occasione o a causa di manifestazioni sportive ed è stato successivamente esteso, dal d.l. n. 14/2017, ai reati commessi con violenza alle persone o alle cose, compiuti alla presenza di più persone anche in occasioni pubbliche, per i quali è obbligatorio l'arresto, e, da ultimo, dal d.l. n. 130/2020 ai reati commessi in occasione o a causa del trattenimento in uno dei centri di permanenza per il rimpatrio (CPR o *hotspot*) o delle strutture di primo soccorso e accoglienza (CPA e CAS). Cfr. S. SIGNORATO, *Arresto in flagranza differita: limiti sistematici e prospettive*, in *Riv. dir. proc.*, 2020; L. DELLA RAGIONE, *Le nuove misure pre-cautelari: l'arresto in flagranza e l'allontanamento d'urgenza dalla casa familiare del P.M.*, in B. ROMANO-A. MARANDOLA (a cura di), *Codice rosso*, II ed., agg. e integr., Pacini, Pisa, 2024, p. 215; P. SPAGNOLO, *Le nuove disposizioni processuali in materia di contrasto alla violenza sulle donne e alla violenza domestica*, in *Leg. pen.*, 2024, p. 14 ss.; L. ALGERI, *L'arresto in flagranza differita per reati di violenza di genere e domestica*, in *Dir. pen. e proc.*, 2024, p. 181 ss.

[97] Affinché tale strumento trovi applicazione, il legislatore ha delineato una serie di condizioni cumulative che ne circoscrivono l'ambito operativo: a) la documentazione su cui si fonda l'arresto deve consistere in videoriprese o contenuti provenienti da dispositivi di comunicazione elettronica o telematica (ad es. SMS, e-mail, messaggi *WhatsApp*), purché formati contestualmente al fatto e spontaneamente acquisiti; b) è richiesta la legittima acquisizione del materiale, non solo in termini di origine lecita, ma anche quanto a verificabilità temporale e di provenienza, al fine di prevenire manipolazioni o interpolazioni che inficerebbero la genuinità della prova; c) deve emergere inequivocabilmente il fatto criminoso, con le sue coordinate essenziali, e l'identità dell'autore, in modo tale che la documentazione costituisca, di per sé, un elemento auto-sufficiente e probante dell'illecito. Cfr. A. MARANDOLA, *Violenza di genere: la Cassazione inizia a definire i contorni dell'arresto differito*, in *Sist. pen.*, 18 ottobre 2024.

apertura implicita all'utilizzo di strumenti tecnici avanzati, qualora essi siano in grado di soddisfare i requisiti di precisione, tempestività e legittimità del dato. In particolare, il quadro delineato sembra ammettere che la polizia giudiziaria possa fondare l'intervento precautelare su evidenze di natura tecnologica, a condizione che rispettino i parametri di liceità sostanziale e processuale, oltre a quelli della pertinenza e della necessità, come imposti dalla normativa sul trattamento dei dati personali e dalle garanzie difensive di matrice costituzionale [98]. In tale cornice, il riconoscimento facciale automatizzato potrebbe, almeno in via teorica, assurgere a uno degli strumenti tecnici in grado di supportare l'accertamento dell'identità del soggetto in tempi compatibili con le esigenze di tempestività dell'arresto *extra-flagranza*, a patto che sia debitamente validato e sottoposto a controllo umano qualificato [99], colmando l'assenza di percezione diretta e, quindi, superando i limiti probatori tipici della "quasi flagranza" [100].

Tuttavia, occorre rilevare come l'ambito applicativo dell'istituto è stato circoscritto a fattispecie incriminatrici che, per loro natura, si articolano in sequenze plurime di condotte, spesso prive di univoca rilevanza autonoma e temporalmente diluite [101]. L'esigenza di accertare l'"attualità" della condotta criminosa, quale presupposto necessario dell'arresto differito, risulta pertanto difficilmente compatibile con la struttura dei reati abituali, per i quali la dimensione cronologica del fatto tipico sfugge a una precisa cristallizzazione in un singolo evento.

Inoltre, il presupposto della riferibilità inequivoca – elemento strutturale dell'art. 382-*bis* c.p.p. – sembra rinviare a un paradigma probatorio che

---

[98] Cfr. A. MARANDOLA, *Violenza di genere: la Cassazione inizia a definire i contorni dell'arresto differito*, cit.

[99] Cfr. A. MARANDOLA, *Violenza di genere: la Cassazione inizia a definire i contorni dell'arresto differito*, cit.

[100] Cfr. D. PERUGIA, *La codificazione dell'arresto in flagranza "differita". Dalla violenza negli stadi alla violenza sulle donne e nei confronti del personale sanitario: esperimenti di prevenzione e repressione di reati*, in *Dir. dif.*, 12 dicembre 2024.

[101] Cfr. artt. 387-*bis*, 572 e 612-*bis* c.p. Ai sensi del comma 1-*bis*, sono stati inclusi anche i delitti non colposi per i quali è previsto l'arresto in flagranza, commessi all'interno o nelle pertinenze delle strutture sanitarie o socio-sanitarie residenziali o semiresidenziali, pubbliche o private, in danno di persone esercenti una professione sanitaria o socio-sanitaria nell'esercizio o a causa delle funzioni o del servizio nonché di chiunque svolga attività ausiliarie di cura, assistenza sanitaria o soccorso, funzionali allo svolgimento di dette professioni, nell'esercizio o a causa di tali attività, ovvero commessi su cose ivi esistenti o comunque destinate al servizio sanitario o socio-sanitario.

presuppone l'utilizzo di documentazione già disponibile e verificata dagli esperti o comunque spontaneamente acquisita al di fuori del procedimento. Si tratterebbe, dunque, di materiale probatorio di natura extraprocedimentale, ottenuto non necessariamente mediante strumenti tecnologici avanzati in grado di associare *in tempo reale* l'identità dei soggetti, comprensivo di una serie di dati e informazioni che ne certifichino l'inequivocabile provenienza e riferibilità. Giova pertanto prendere atto che la nozione di «documentazione legittimamente ottenuta da dispositivi di comunicazione informatica o telematica» di cui all'art. 382-*bis*, comma 1, c.p.p. è alquanto generica e destinata a ricomprendere qualunque strumento di natura tecnologica [102]. Nello specifico, con riferimento ai delitti di cui al comma 1, trattandosi di reati le cui condotte vengono poste in essere all'interno delle mura domestiche, e che, pertanto, possono concretizzarsi in appostamenti o chiamate e messaggi ripetuti, è dato ipotizzare che gli strumenti di comunicazione informatica o telematica, da cui si ricavano i dati digitali rappresentati da messaggi di testo o multimediali, video, foto, e-mail o tabulati telefonici, possano venire individuati tra *smartphone*, *iPads*, computer [103]. Analoga considerazione vale per i delitti sottesi alla previsione di cui all'art. 382-*bis*, comma 1-*bis*, c.p.p. – che, commessi all'interno delle strutture sanitarie pubbliche o private, possono essere ripresi da telecamere a circuito chiuso o, presumibilmente, da *smartphones* di persone presenti all'interno delle stesse strutture. In questo contesto, le maggiori preoccupazioni sono legate all'acquisizione non genuina del materiale digitale proveniente dal dispositivo elettronico, essendo tale documentazione per natura volatile e suscettibile di continua trasformazione [104]. Il che conferma la necessità di un'accurata verifica in ordine alla genuinità dell'acquisizione del materiale informatico, onde assicurare «che la riproduzione … sia fedele alla matrice digitale e, come tale, idonea a garantire un accertamento attendibile dei fatti rappresentati» [105]. In tal senso, l'organo giudicante è investito del compito di effettuare

---

[102] D. PERUGIA, *La codificazione dell'arresto in flagranza "differita". Dalla violenza negli stadi alla violenza sulle donne e nei confronti del personale sanitario: esperimenti di prevenzione e repressione di reati*, cit.

[103] D. PERUGIA, *La codificazione dell'arresto in flagranza "differita". Dalla violenza negli stadi alla violenza sulle donne e nei confronti del personale sanitario: esperimenti di prevenzione e repressione di reati*, cit.

[104] Cfr. *supra* il § 3.

[105] Cfr. G. FIORELLI, *Lo screenshot quale prova documentale: regole acquisitive e garanzie di affidabilità*, in *Dir. internet*, 3, 2020, p. 507.

un rigoroso scrutinio sugli allegati prodotti, al fine di accertare la sussistenza di quei presupposti oggettivi e soggettivi del reato che, pur in assenza di una percezione diretta dell'illecito, risultano ricostruibili sulla base di evidenze tecnico-documentali. Tale controllo giurisdizionale non si risolve in un mero riscontro formale della regolarità procedurale dell'arresto, ma implica una valutazione sostanziale dell'affidabilità, coerenza e riferibilità probatoria del materiale acquisito che deve essere in grado di rappresentare con chiarezza l'accadimento criminoso e la sua immediata attribuibilità al soggetto sottoposto alla misura. Si tratta di un'operazione che richiama il canone dell'"inequivocabilità" come criterio normativo selettivo e altamente restrittivo, volto a delimitare l'ambito applicativo dell'istituto a sole ipotesi dotate di chiara evidenza probatoria.

In quest'ottica, è dubbio che la norma in esame possa fungere da base giuridica idonea a legittimare l'impiego sistematico di strumenti di riconoscimento facciale *in tempo reale*, i quali come visto – per la loro intrinseca invasività e per il rischio di lesione della libertà personale e del diritto alla riservatezza – necessitano di uno specifico fondamento giuridico [106]. Sebbene non si possa escludere del tutto un futuro innesto interpretativo volto a ricomprendere anche l'*output* dei sistemi biometrici ottenuti in tempo reale nell'alveo dell'art. 382-*bis* c.p.p., tale operazione ermeneutica risulterebbe – allo stato – scarsamente sostenibile, sia sul piano testuale, a causa dell'incertezza rappresentativa e dell'attuale difficoltà di dimostrare il perché del raggiungimento di un determinato risultato, sia alla luce dei principi costituzionali e sovranazionali in materia di tutela dei diritti fondamentali [107]. L'esclusione si impone infatti in tutte le ipotesi in cui la dimostrazione di un fatto o dell'identità di un soggetto si fondi su tecnologie la cui logica operativa risulti intrinsecamente non intellegibile e, dunque, refrattaria a un controllo epistemologicamente verificabile da parte dell'autorità giudiziaria, come invece richiesto in questo caso. In altre parole, la non spiegabilità dell'*output* generato dal sistema impedisce l'assunzione del risultato come dato probatorio idoneo a fondare una misura gravemente lesiva della libertà personale, quale l'arresto in flagranza differita ai sensi dell'art. 382-*bis c*.p.p.

Rimanendo sempre in tema di videoriprese, ulteriori spunti di riflessione possono essere desunti dal contributo della giurisprudenza che, nel tempo, ha

---

[106] Cfr. il capitolo III.

[107] Cfr. il capitolo III. In questo senso anche S. SIGNORATO, *Arresto in flagranza differita: limiti sistematici e prospettive*, in *Riv. dir. proc.*, 2020, p. 87.

progressivamente delineato i contorni applicativi e le condizioni di legittimità dell'utilizzo di tali strumenti nel contesto del procedimento penale. Si è già fatto brevemente richiamo alla famosa sentenza Prisco[108] che, nel fornire un'interpretazione sistematica dell'impiego dei filmati per scopi processuali, ha concluso che le videoregistrazioni eseguite in luoghi pubblici, effettuate al di fuori dell'ambito del procedimento penale, vadano incluse nella categoria dei documenti di cui all'art. 234 c.p.p.[109], mentre, se eseguite dalla polizia giudiziaria, a procedimento penale avviato, vadano annoverate entro la categoria delle prove atipiche, sempre se rispettose del duplice requisito dell'*idoneità* ad assicurare l'accertamento del fatto e dell'*assenza di un pregiudizio per la libertà morale* della persona[110] e la cui legittimità è subordinata alla sussistenza di un'autorizzazione motivata da parte dell'autorità giudiziaria, funzionale a garantirne la conformità ai principi di legalità, proporzionalità e necessità. Di qui, le operazioni eseguite all'interno del domicilio, o in luoghi assimilabili ad esso[111], sono state inquadrate diversamente a seconda che l'oggetto ritragga comportamenti "comunicativi" o "non comunicativi". È stato in particolare escluso che ambienti quali i *privé* di locali notturni o i servizi igienici pubblici, benché destinati a momenti di riservatezza individuale, possano essere ricompresi nella nozione costituzionale di domicilio ai sensi dell'art. 14 Cost., in quanto privi di quella stabile connessione identitaria e funzionale con la persona che consente di sottrarre l'ambiente a indebite ingerenze esterne indipendentemente dalla presenza fisica

---

[108] Già richiamata al § 2. Cfr. Cass. pen., S.U., 28 marzo 2006, n. 26795, in *CED Cass.*, n. 234270. Sul punto v. C. CONTI, *Le video-riprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi "riservati"*, in *Dir. pen. e proc.*, 11, 2006, p. 1347 ss.; C. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen. e proc.*, 9, 2018, p. 1211; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 303 ss.; F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Wolter Kluwer, Milano, 2020, p. 29 ss.; G. DI PAOLO, *"Tecnologie del controllo" e prova penale. L'esperienza statunitense e spunti per la comparazione*, Cedam, Padova, 2008, p. 186 ss.; A. CAMON, *Le Sezioni Unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi*, in *Riv. it. dir. proc. pen.*, 2006, p. 1550; C. RIZZO, *Videoriprese in luoghi pubblici e poteri degli organi di polizia*, in *Cass. pen.*, 11/2024, p. 3584.

[109] Cfr. Cass. pen., S.U., 28 marzo 2006, n. 26795, cit., § 4.

[110] Art. 189 c.p.p. Per una ricostruzione analitica cfr. G. DI PAOLO, *"Tecnologie del controllo" e prova penale*, cit., p. 188 eL. CUOMO, *La prova digitale*, in G. CANZIO-L. LUPARIA (a cura di), *Prova scientifica e processo penale*, Wolters Kluwer Cedam, Milano, 2018, p. 738.

[111] Cfr. G. DI PAOLO, *"Tecnologie del controllo" e prova penale*, cit., p. 227 ss.

dell'interessato [112]. In tali luoghi, la videoregistrazione di comportamenti privi di contenuto comunicativo – ovvero atti non finalizzati alla trasmissione di un pensiero mediante parole, gesti, espressioni o atteggiamenti – è stata ritenuta legittima se autorizzata dal pubblico ministero e, in quanto prova atipica, liberamente valutabile dal giudice di merito.

Di contro, quando la videoripresa abbia ad oggetto comportamenti comunicativi, anche se effettuata in spazi non riconducibili alla nozione di domicilio, l'attività di captazione assume natura intrusiva al pari di una intercettazione ambientale, con la conseguente necessità dell'autorizzazione da parte del giudice ai sensi degli artt. 266 ss. c.p.p. Ne deriva un regime differenziato fondato non soltanto sul tipo di ambiente in cui avviene la registrazione, ma soprattutto sulla natura comunicativa o meno dell'atto oggetto di osservazione [113]. Come è stato osservato, il confine tra meri comportamenti (azioni come ad esempio il confezionamento della droga) e comunicazioni (anche non verbali, come nel caso di gesti o smorfie) può rivelarsi oltremodo labile, sicché l'utilizzabilità della prova viene ad essere ancorata a parametri evanescenti e impercettibili [114]; senza contare che tale distinzione si confronta con l'impossibilità pratica di differenziare *ex ante* i diversi tipi di comportamenti.

Alla luce dell'interpretazione richiamata, i sistemi di riconoscimento facciale *in tempo reale*, configurandosi come forma di "videoripresa algoritmica"

---

[112] Cfr. *ex multis* Cass. pen., sez. II, 22 maggio 2018, n. 22972; Cass. pen., sez. VI, 12 dicembre 2016, n. 52595; Cass. pen., sez. V, 3 giugno 2015, n. 11419; Cass. pen., sez. VI, 12 luglio 2013, n. 30177; Cass. pen., sez. VI, 5 settembre 2012, n. 33593; Cass. pen., sez. I, 19 gennaio 2009, n. 4422; Cass. pen., sez. V, 3 ottobre 2008, n. 37698.

[113] Nella pronuncia delle sezioni unite emerge con chiarezza il divieto assoluto di videoregistrazioni – anche di comportamenti non comunicativi – all'interno del domicilio, in quanto lesive del diritto costituzionalmente garantito all'inviolabilità del domicilio *ex* art. 14 Cost. In tale ipotesi, le immagini ottenute in violazione della suddetta garanzia configurano prove illecite, la cui inutilizzabilità si estende anche alla fase cautelare del procedimento. L'atto risulta poi svincolato dal rispetto di particolari formalità esecutive ove abbia ad oggetto condotte non comunicative che hanno luogo in spazi pubblici ovvero aperti o esposti al pubblico. Cfr. G. DI PAOLO, *"Tecnologie del controllo" e prova penale*, cit., p. 225; L. CUOMO, *La prova digitale*, in G. CANZIO-L. LUPARIA (a cura di), *Prova scientifica e processo penale*, Wolters Kluwer Cedam, Padova, 2018, p. 739 e A. CABIALE, *I limiti alla prova nella procedura penale europea*, Wolters Kluwer Cedam, Milano, 2020, p. 40 ss.

[114] Cfr. A. CAMON, *Le Sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi*, in *Riv. it. dir. proc. pen.*, 2006, p. 1550 e O. MAZZA, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Dir. pen. cont.-Riv. trim.*, 3, 2013, p. 10 ss.

priva della finalità volta alla captazione di condotte comunicative, non risultano suscettibili di essere ricondotti, attraverso un'interpretazione analogica, alla disciplina prevista per le intercettazioni di comunicazioni [115]. Tale attività si differenzia ontologicamente dalle intercettazioni, in quanto non implica l'invasione di uno spazio comunicativo privato, né presuppone l'acquisizione di informazioni attinenti alla sfera dialogica e relazionale dell'individuo. Al contrario, il riconoscimento facciale si sostanzia in una procedura digitale di estrazione e trattamento sistematico di dati biometrici «non comunicativi», operata attraverso strumenti di elaborazione automatica, privi di finalità di ascolto o registrazione di conversazioni.

Né tali strumenti potrebbero essere inquadrati più semplicemente fra i documenti, dal momento che non si limitano a catturare e a registrare passivamente le immagini ritraenti i volti, ma implicano un'elaborazione finalizzata a generare un esito identificativo immediato. Questo elemento distintivo li rende assimilabili a meccanismi di elaborazione di dati automatizzati piuttosto che a meri documenti nel senso tradizionale del termine. Infatti, come anticipato *supra*, un documento in senso processuale viene generalmente inteso come un supporto materiale o digitale che riproduce un'informazione statica e precostituita [116], mentre il riconoscimento facciale *in tempo reale* genera un *output* dinamico, ossia un esito di una comparazione, frutto di un processo computazionale autonomo che incide direttamente sulle attività di acquisizione e utilizzo dell'informazione.

Nondimeno, per le stesse ragioni già formulate per l'impiego del sistema *a posteriori*, difficilmente questa modalità applicativa potrebbe trovare terreno fertile con l'applicazione dell'art. 189 c.p.p., tradizionalmente inteso quale *passe-partout* per l'ammissione di mezzi di prova e di mezzi di ricerca della prova atipici [117]. Infatti, l'autorità giudiziaria non risulta in grado di valutare l'effettiva idoneità dei sistemi di riconoscimento facciale *in tempo reale* a garantire un accertamento probatorio attendibile. Tale difficoltà, come visto, è imputabile alla strutturale opacità che caratterizza questi strumenti,

---

[115] Cfr. J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, in I. MICHELI (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*, EUT Edizioni Università di Trieste, Trieste, 2023, p. 174.

[116] Cfr. F. ZACCHÉ, *La prova documentale*, Giuffrè, Milano, 2012, p. 7 ss. Cfr. *supra* il § 3.

[117] M. GIALUZ, *Premessa*, in *Diritto di Internet Digital Copyright e Data Protection*, 1, 2020, p. 6.

derivante dalla complessità dei modelli sottostanti [118]. Inoltre, risulta emblematico il fatto che, anche con riferimento a questa modalità applicativa, nonostante siano trascorsi diversi anni dalla sua implementazione tecnica, continuino a mancare informazioni cruciali per una comprensione esaustiva delle caratteristiche operative e dei criteri decisionali che ne regolano il funzionamento, precludendone così un controllo effettivo.

Anche volendo guardare ai criteri elaborati dai più recenti orientamenti giurisprudenziali in materia di mezzi atipici di ricerca della prova, emergono rilevanti criticità in relazione alla loro possibile estensione interpretativa ai sistemi di riconoscimento facciale *in tempo reale.* Infatti, la giurisprudenza in materia di pedinamento elettronico tramite GPS ha giustificato l'applicabilità dell'art. 189 c.p.p. sulla base dell'assenza di un accumulo massivo di dati sensibili da parte del fornitore del servizio, con la conseguenza che le relative risultanze probatorie possono essere acquisite senza la necessità di una preventiva autorizzazione dell'autorità giudiziaria [119]. Considerando i diversi sistemi di riconoscimento facciale *in tempo reale*, il criterio individuato risulta difficilmente applicabile. Oltre alle già complesse problematiche legate alla non spiegabilità intrinseca del funzionamento di tali software [120], permane l'incertezza tecnica circa le modalità di gestione delle informazioni biometriche catturate. In particolare, non è chiaro se tali sistemi si limitino sempre a elaborare e conservare esclusivamente i dati relativi ai volti per i quali viene riscontrata una corrispondenza positiva con le banche dati di riferimento [121], oppure se, al contrario, gli strumenti memorizzino indiscriminatamente i volti di tutti i soggetti inquadrati dalle

---

[118] Cfr. il capitolo III, § 5.

[119] Cfr. *ex multis* Cass. pen. 18 settembre 2024, n. 37395, in *CED Cass.*, n. 286949, Cass. pen. 9 marzo 2023, n. 15422, in *CED Cass.*, n. 284582. Per un approfondimento, cfr. C. FANUELE, *La localizzazione satellitare nelle investigazioni penali*, Wolters Kluwer Cedam, Milano, 2019.

[120] Cfr. il capitolo III, § 5.

[121] Nel caso inglese richiamato al capitolo III, § 4.3, lo strumento era stato progettato in modo da registrare e conservare esclusivamente i riscontri positivi (*positive matches*) tra i dati biometrici acquisiti *in tempo reale* e quelli presenti nelle banche dati di riferimento. Contestualmente, il sistema prevedeva la cancellazione automatica e immediata di tutte le ulteriori informazioni raccolte che non generavano corrispondenze significative, evitando così l'accumulo di dati relativi a soggetti estranei alle finalità investigative. In assenza di dati specifici, risulta complesso formulare generalizzazioni attendibili, considerando la possibilità che le tecnologie impiegate presentino caratteristiche eterogenee e variabili in funzione del contesto di applicazione.

telecamere. Tale distinzione, tutt'altro che marginale, rappresenta un elemento dirimente ai fini del rispetto dei principi fondamentali in materia di protezione dei dati personali, in particolare dei principi di minimizzazione e di proporzionalità [122]. L'ipotesi di un trattamento selettivo e mirato, limitato ai soli dati correlati a un *match* positivo, garantirebbe, in astratto, una maggiore conformità ai parametri di necessità e adeguatezza, attenuando l'invasività dell'intervento tecnologico nella sfera privata degli individui estranei all'indagine.

A sua volta, anche il requisito del rispetto della libertà morale dell'individuo potrebbe non risultare adeguatamente salvaguardato [123]. I sistemi di riconoscimento facciale *in tempo reale* non si limitano a elaborare i dati in modo neutro, ma estraggono informazioni dal "corpo digitalizzato" della persona, incidendo in modo significativo sul diritto all'autodeterminazione informativa e inibendo la libera espressione di comportamenti individuali e sociali, ovvero, determinando una forma di condizionamento latente delle abitudini quotidiane. Tale effetto dissuasivo, ancorché indiretto, configura una compressione della libertà personale e relazionale con implicazioni rilevanti per la tenuta complessiva della garanzia.

Nella prospettiva che caratterizza questa analisi – ovvero l'individuazione delle direttrici che dovrebbero ispirare un'adeguata disciplina normativa della materia che qui si tratta – si devono prevenire i rischi di violazione della libertà morale, della privacy e del diritto della riservatezza dell'individuo [124] e dunque, in breve, di utilizzo di una *prova incostituzionale* [125]. È ampiamente

---

[122] Cfr. il capitolo III, § 4 ss.

[123] Cfr. più ampiamente il capitolo III, § 2.

[124] Cfr. il capitolo III, § 4.

[125] Per un'articolata esposizione sul tema si rinvia *ex multis* a P. TONINI-C. CONTI, *Il diritto delle prove penali*, cit., p. 201 ss., N. GALANTINI, voce *Inutilizzabilità*, in *Enc. dir.*, Agg. I, Milano, 1997, p. 700; G. ILLUMINATI, *L'inutilizzabilità della prova nel processo penale italiano*, in *Riv. it. dir. e proc. pen.*, 2010, p. 534 ss.; S. MARCOLINI, *Regole di esclusione e nuove tecnologie*, in *Criminalia*, 1, 2006, p. 419; C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Cedam, Padova, 2007; E.N. LA ROCCA, voce *Inutilizzabilità*, in *Dig. disc. pen.*, Agg. I, Torino, 2008, p. 613 ss.; A. SCELLA, *L'inutilizzabilità della prova nel sistema del processo penale*, in *Riv. it. dir. e proc. pen.*, 1992, p. 203 ss.; P. NUVOLONE, *Le prove vietate nel processo penale nei paesi di diritto latino*, in *Riv. dir. proc.*, 1966, p. 442 ss.; F. CAPRIOLI, *Colloqui riservati e prova penale*, Giappichelli, Torino, 2000, p. 236 ss.; F. M. GRIFANTINI, *Il segreto difensivo nel processo penale*, Giappichelli, Torino, 2001, p. 279 ss.; A. CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen.*, 1999, p. 1196 ss.; G. SPANGHER, *«E pur si muove» dal male captum bene retentum alle*

noto in dottrina e giurisprudenza che la questione dell'ammissibilità di tale prova, in quanto acquisita in violazione immediata e diretta dei diritti fondamentali della persona, non abbia ancora raggiunto una definizione stabile e condivisa, né sotto il profilo teorico, né sul piano applicativo. L'interpretazione, di particolare complessità sistematica, risulta al centro di un vivace dibattito scientifico, all'interno del quale si sono delineati, in via ricostruttiva, alcuni orientamenti, ciascuno dei quali fornisce differenti coordinate metodologiche per affrontare il tema della rilevanza probatoria di atti lesivi di prerogative costituzionalmente garantite [126].

Con l'avvertenza metodologica che una sintesi eccessiva rischia di comprimere la varietà e la profondità delle elaborazioni teoriche maturate in merito, si può segnalare, quale primo approccio, la teoria della *tutela diretta del diritto fondamentale*, secondo la quale sarebbe possibile ricavare direttamente dalla Costituzione una regola di esclusione probatoria, la quale renderebbe inutilizzabile la prova ottenuta mediante la violazione di un diritto inviolabile. Tale ricostruzione si ispira al paradigma statunitense della *exclusionary rule*, come pure alla dottrina dei *fruits of the poisonous tree* [127], secondo cui la prova, se derivante da una condotta incostituzionale, è da considerarsi radicalmente inutilizzabile. Questa impostazione, sebbene non esplicitamente recepita nel sistema processuale italiano, ha ricevuto riconoscimenti giurisprudenziali parziali. In particolare, com'è noto, nella sentenza n. 34/1973, la Corte costituzionale ha osservato che le attività poste in essere in violazione dei diritti fondamentali non possono legittimare atti processuali basati su tali condotte, affermazione che, sebbene inserita in forma di *obiter dictum*, rivela un'apertura verso una possibile esclusione automatica della prova incostituzionale [128].

Un secondo e autorevole orientamento si fonda sull'assunto per cui non sarebbe possibile desumere, in via interpretativa, dalla previsione costituzionale di un diritto fondamentale una regola di esclusione probatoria, tale da

---

esclusionary rules, in *Giur. cost.*, 2001, p. 2829 ss.; C. CONTI, *Il principio di non sostituibilità: il sistema probatorio tra costituzione e legge ordinaria*, in *Cass. pen.*, 2, 2024, p. 451.

[126] Per una ricostruzione esaustiva si rinvia a G. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*, in *Cass. pen.*, 2, 2025, p. 638 e P. TONINI-C. CONTI, *Il diritto delle prove penali*, cit., p. 104 ss.

[127] In argomento, R. CASIRAGHI, *Prove vietate e processo penale*, in *Riv. it. dir. proc. pen.*, 2009, p. 1787.

[128] Corte cost. 6 aprile 1973, n. 34, in *Giur. cost.*, 1973, p. 331 ss., con nota di V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche.*

impedire l'ammissione e l'acquisizione della prova medesima, in assenza di una specifica disposizione del codice di rito [129]. Secondo tale impostazione, i soli limiti alla formazione probatoria cui fa riferimento l'art. 191 c.p.p. troverebbero fondamento esclusivamente nel diritto processuale positivo, con la conseguenza che l'inosservanza di norme di rango costituzionale non comporterebbe *ex se* l'inutilizzabilità della prova, ma richiederebbe l'attivazione del controllo di costituzionalità sulla disposizione processuale che ne consente l'ammissione. Sulla base di questa ricostruzione, dunque, il giudice, ove si trovi dinanzi a una norma processuale astrattamente idonea a legittimare l'introduzione nel processo di una prova in contrasto con un diritto fondamentale, sarebbe tenuto a sollevare questione di legittimità costituzionale, promuovendo il vaglio del Giudice delle leggi, affinché quest'ultimo valuti l'eventuale illegittimità della disposizione. Questo approccio postula una forma di tutela indiretta del diritto costituzionale leso, rimessa all'intervento successivo della Corte costituzionale.

In posizione intermedia tra la tutela diretta e quella indiretta, si colloca una terza impostazione. Tale filone interpretativo ammette la possibilità per l'interprete di evitare la declaratoria di illegittimità costituzionale di una norma processuale attraverso un'operazione esegetica, volta a colmare eventuali lacune di garanzia [130]. A tal fine, si prospetta la necessità di desumere analogicamente dalla Costituzione – ovvero dalle norme processuali che disciplinano fattispecie analoghe – un nucleo essenziale di garanzie che possa rendere conforme al dettato costituzionale la disciplina processuale in esame [131]. Seguendo quest'ultima impostazione ermeneutica, il giudice del dibattimento, investito della richiesta di ammissione di una prova atipica, quale il risultato di un'attività di riconoscimento facciale automatizzato, sarebbe tenuto a compiere una valutazione preliminare di ammissibilità

---

[129] Cfr. F. CORDERO, *Prove illecite nel processo penale*, in *Jus*, 1961, p. 73 ss.; ID., *Il procedimento probatorio*, in *Tre studi sulle prove penali*, Giuffrè, Milano, 1963.

[130] Cfr. D. ZIGNANI, *Una discutibile pronuncia in tema di prove illegittimamente carpite nel domicilio*, in *Cass. pen.*, 2004, p. 1316.

[131] Tale approccio è rinvenibile nella sentenza n. 81/1993 della Corte costituzionale, nella quale si è affermata la necessità di una previa autorizzazione giudiziale per l'acquisizione dei dati esterni relativi al traffico telefonico, anche in assenza di una previsione normativa espressa, derivando tale esigenza direttamente dall'art. 15 Cost., Corte cost. 11 marzo 1993, n. 81, in *Giur. cost.*, 1993, p. 731 ss. Cfr. anche Cass. pen., S.U., 28 marzo 2006, n. 26795, Prisco, in *Cass. pen.*, 2006, p. 4344, con nota di M.L. Di BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni unite.*

connotata da un'estensione e una profondità superiori rispetto a quella normalmente richiesta per le prove tipiche previste dal codice di rito. Tale scrutinio si fonda sulla necessaria verifica della conformità dell'attività probatoria proposta non solo alle regole strettamente processuali. In base a questa impostazione, non può considerarsi *non disciplinata dalla legge* – e dunque ammissibile quale prova atipica *ex* art. 189 c.p.p. – un'attività probatoria che, per le sue modalità di acquisizione o per gli effetti che produce, risulti vietata seguendo i principi generali dell'ordinamento [132]. Questo criterio, che postula l'inammissibilità di mezzi probatori fondati su condotte vietate o su atti intrinsecamente illeciti, si rivela di particolare interesse con riferimento all'impiego processuale dei sistemi di riconoscimento facciale. In tale contesto, infatti, qualora il trattamento automatizzato dei dati biometrici risulti privo di base legale adeguata o si configuri come contrario ai principi di liceità, correttezza, trasparenza, proporzionalità e minimizzazione dei dati [133] potrebbe dar luogo a una incompatibilità tra l'attività di *facial recognition* e l'ammissione della relativa prova [134].

L'elaborazione dottrinale che esige la verifica della liceità del mezzo impiegato per l'acquisizione del dato probatorio impone, dunque, una rigorosa verifica non solo dell'affidabilità tecnica dello strumento, ma anche della conformità del trattamento dei dati biometrici ai presidi giuridici posti a tutela della riservatezza e dell'identità personale. In assenza di uno specifico apparato normativo chiaro, puntuale e proporzionato, idoneo a regolare le condizioni, i limiti e le garanzie nell'utilizzo dei sistemi di riconoscimento facciale, l'impiego di tali tecnologie potrebbe risultare inammissibile come prova. In tal senso, alla luce della predetta interpretazione sistematica dell'art. 189 c.p.p., l'illiceità del trattamento assume funzione escludente, costituendo limite ineludibile all'ingresso della prova nel processo, a prescindere dalla rilevanza o dalla potenziale utilità del risultato di compatibilità biometrica. Tale conclusione, lungi dal rappresentare un'irragionevole restrizione dell'accertamento penale, si configura quale espressione del principio di legalità della prova, a presidio della dignità e dei diritti fondamentali della persona.

---

[132] Cfr. P. TONINI-C. CONTI, *Il diritto delle prove penali*, cit., p. 203 ss.

[133] In quanto espressione della normativa sulla protezione dei dati personali, il diritto alla riservatezza è stato progressivamente interpretato come una manifestazione essenziale della dignità e dell'autodeterminazione della persona, al punto da essere ricondotto al novero dei diritti fondamentali tutelati dall'art. 2 della Costituzione. Cfr. il capitolo III, § 4 ss.

[134] In tal senso, cfr. A. MARANDOLA, *Il riconoscimento facciale*, cit., p. 511 e J. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., p. 1081.

In considerazione di quanto detto e in assenza delle necessarie informazioni sulle effettive capacità tecniche di questi strumenti, le operazioni di riconoscimento eseguite mediante sistemi di riconoscimento facciale *in tempo reale* a fini probatori devono considerarsi radicalmente inibite [135]. L'unico assetto tecnologico compatibile con il rispetto dei diritti fondamentali appare essere quello in cui l'impiego dei sistemi di riconoscimento facciale *in tempo reale* sia limitato, in modo rigoroso e non derogabile, al trattamento e alla conservazione esclusiva dei soli dati biometrici che abbiano generato un riscontro positivo con le immagini archiviate nelle banche dati di riferimento e sia impiegato unicamente come mezzo di ausilio per le attività di identificazione dell'art. 349 c.p.p. In tal senso, ogni trattamento ulteriore di dati relativi a soggetti estranei – ovvero privi di corrispondenza – dovrebbe essere considerato non conforme al principio di minimizzazione [136]. Inoltre, dal punto di vista epistemologico, l'*output* di un sistema di riconoscimento facciale *in tempo reale* non è in grado di fornire certezza circa la presenza di un determinato soggetto in un determinato luogo e tempo. Esso, piuttosto, rappresenta una mera inferenza probabilistica – espressa spesso sotto forma di percentuale di compatibilità biometrica – il cui significato deve essere interpretato alla luce di un'adeguata analisi contestuale.

L'adozione di una simile architettura tecnica, tuttavia, non pare essere sufficiente in sé a garantire il rispetto dei valori di uno Stato di diritto. Occorre, infatti, predisporre a livello nazionale un sistema di autorizzazione preventiva, che subordini l'attivazione di tali sistemi a un vaglio rigoroso da parte dell'autorità giudiziaria, con indicazione dettagliata delle finalità perseguite, dei luoghi di utilizzo, della durata e dei soggetti sottoposti a monitoraggio.

È altresì indispensabile introdurre meccanismi di controllo successivo e periodico, nonché procedure di verifica dell'effettiva conformità dei sistemi agli standard previsti, anche mediante *audit* indipendenti e un accesso pubblico ai report sull'utilizzo della tecnologia. L'obiettivo di tali garanzie è evitare qualunque slittamento verso forme di sorveglianza generalizzata, incompatibili con i principi dell'ordinamento democratico e con le garanzie del giusto processo, assicurando che l'impiego della tecnologia non si traduca in

---

[135] Cfr. J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, cit., p. 175.

[136] Cfr. il capitolo III, § 4.2.

una compressione sistematica della libertà personale, della riservatezza e del diritto di difesa [137]. Non è sufficiente al raggiungimento di tale standard di garanzia, il complesso apparato di divieti ed eccezioni poste dall'art. 5 del regolamento 2024/1689: come in precedenza illustrato, la vaghezza e la genericità delle eccezioni previste dall'art. 5, lett. h) al divieto generale impedisce a tale disposizione di configurarsi come un completo schema di regole per la costruzione di un'adeguata base normativa.

6. *La capacità dimostrativa di un* match *biometrico*

Con l'obiettivo di individuare un sistema di regole nazionali ispirate ai principi introdotti e consolidati a livello europeo [138], i temi che si presentano come oggetto centrale della riflessione concernono la capacità dimostrativa di un *match* generato da uno strumento computazionale di riconoscimento facciale (sia *a posteriori*, sia *in tempo reale*) e la valutazione della sua attendibilità.

L'indagine si concentra in primo luogo sull'effettiva funzione informazionale di tali risultati e sul loro contributo conoscitivo per l'accertamento dei fatti. Ci si propone, dunque, di valutare se e in che misura tali risultati – in quanto *output* algoritmici derivanti da processi di comparazione automatizzata – possano fornire un contributo valido alla ricostruzione dell'evento storico oggetto del procedimento penale.

In un'ottica metodologicamente consapevole e coerente con l'approccio analitico adottato nel presente studio, appare opportuno premettere che le riflessioni che seguono non si propongono di apportare un contributo sistematico alla ricostruzione teorica del concetto di prova – da sempre oggetto di uno dei dibattiti più densi e raffinati della dottrina processualpenalistica – ma si collocano in una prospettiva funzionale, volta a enucleare taluni snodi concettuali che si rivelano essenziali per lo sviluppo del tema specifico affrontato nel presente lavoro.

---

[137] Cfr. P. DE HERT-G. BOUCHAGIAR, *European Biometric Surveillance, Concrete Rules, and Uniform Enforcement Beyond Regulatory Abstraction and Local Enforcement*, in R. MATULIONYTE-M. ZALNIERIUTE (eds.), *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge University Press, Cambridge, 2024.

[138] Più ampiamente cfr. il capitolo VI.

Assunto condiviso e punto di partenza imprescindibile è l'idea secondo cui la prova rappresenta il veicolo attraverso il quale il processo penale persegue il proprio fine ultimo: la ricostruzione del fatto storico e la formazione del convincimento del giudice. In assenza di una definizione normativa, essa può essere intesa come «ogni dato che, legittimamente acquisito al processo, sia valutabile dal giudice in ordine a una determinata proposizione da provare», oppure, «quanto si assume a dimostrazione di un accadimento e/o delle sue modalità specifiche» [139].

Nel solco di tale premessa, in considerazione delle peculiarità tecniche degli strumenti in esame, si rende utile – pur senza pretesa di esaustività ricostruttiva – richiamare la distinzione teorica tra prova "diretta" o "rappresentativa", in cui tra la proposizione probatoria e il fatto da provare non si interpongono proposizioni intermedie, e prova "indiretta" o "critica", caratterizzata dalla presenza di proposizioni mediate tra l'oggetto della prova e il fatto noto [140]. L'elemento distintivo fra le due categorie concerne essenzialmente il grado di riferibilità al *thema probandum* principale, quale risulta dall'art. 187 c.p.p. Da un lato, le prove dirette o rappresentative si caratterizzano per la loro immediata riferibilità al fatto principale da dimostrare, configurandosi come strumenti cognitivi che offrono una rappresentazione diretta della realtà storica rilevante ai fini del giudizio [141]. Dall'altro lato, le

---

[139] Cfr. *ex multis* P. FERRUA, *La prova nel processo penale*, vol. I, *Struttura e procedimento*, II ed., Giappichelli, Torino, 2017; P. FERRUA, *Teorie della prova: dialogo con Franco Cordero*, in *www.discrimen.it*, 16 dicembre 2020, p. 4 ss.; F. CORDERO, *Procedura penale*, Giuffrè, Milano, 2003, p. 570; F. CORDERO, *Tre studi sulle prove penali*, Giuffrè, Milano, 1963, p. 52, ove l'Autore la definisce «ciò che si usa al fine di provare»; G. UBERTIS, *La conoscenza del fatto nel processo penale*, Giuffrè, Milano, 1992; M. NOBILI, *Concetto di prova e regime di utilizzazione degli atti nel nuovo codice di procedura penale*, in *Foro it.*, 1989, c. 274; M. NOBILI, *Il nuovo 'diritto delle prove' ed un rinnovato concetto di prova*, in *Leg. pen.*, 1989, p. 395 ss.; M. CHIAVARIO, *Considerazioni sul diritto alla prova*, in A. GAITO (a cura di), *Studio sul processo penale in ricordo di Assunta Mazzarra*, Cedam, Padova, 1996, p. 27 ss.; P. TONINI, *La prova penale*, Cedam, Padova, 2000; Cfr. P. TONINI-C. CONTI, *Il diritto delle prove penali*, cit., p. 45; G. UBERTIS, *La prova penale. Profili giuridici ed epistemologici*, Giappichelli, Torino, 1995; G. CARLIZZI, *Morfologia della prova giudiziaria nell'ordinamento italiano*, in A. CARRATTA-M. DE CARO-G. PINO (a cura di), *Intorno al ragionamento giuridico*, Romatre-Press, Roma, 2022, p. 61.

[140] Cfr. F. CARNELUTTI, *Principi del processo penale*, Morano, Napoli, 1960, p. 162 s.; ID., *Diritto e processo*, Morano, Napoli, 1958, p. 129 ss.; G. UBERTIS, *La prova penale. Profili giuridici ed epistemologici*, Utet, Torino, 1995, p. 42; L. SAPONARO, *Dall'indizio alla prova indiziaria: il rapporto tra probabilità e certezza*, Wolters Kluwer Cedam, Milano, 2015.

[141] «Rappresentare un fatto significa costruirne uno equivalente, in modo da renderlo

prove indirette o indiziarie si distinguono per la loro natura derivata, in quanto non attestano il fatto principale in modo immediato, ma si limitano a fornire elementi da cui inferire, mediante un processo logico-deduttivo, l'esistenza del fatto medesimo [142].

Posta questa distinzione, viene spontaneo domandarsi come si collochi il risultato di compatibilità espresso in termini probabilistici di un software di riconoscimento facciale. Cosa rappresenta un *match* rispetto ai fatti oggetto di prova?

Si consideri, a titolo esemplificativo la seguente situazione:

1. Caio è stato vittima di un omicidio in un parco (fatto principale);
2. un soggetto Ignoto viene ripreso dalle telecamere di videosorveglianza all'uscita del medesimo parco (fatto secondario 1);
3. una compatibilità dell'80% tra le immagini di Tizio (sospettato) e Ignoto è stata rilevata da un sistema di riconoscimento facciale (fatto secondario 2).

La circostanza che Tizio e Ignoto siano stati riconosciuti dalla macchina come compatibili all'80% è idonea a inferire un collegamento probatorio significativo con il fatto principale? In effetti, il risultato di compatibilità fra i due dati non è direttamente riferibile al *thema probandum* principale (l'omicidio), ma rappresenta un dato che necessita di altri elementi per essere collegato al fatto storico da provare (Tizio e Ignoto sono simili all'80% (1); l'identità di Tizio e quella di Ignoto coincidono (2); Tizio è l'autore del reato (3)). Il ragionamento che eventualmente collega la compatibilità biometrica e la responsabilità penale di Tizio richiede un insieme di operazioni deduttive: non solo si deve accertare l'assunto che l'individuo ripreso dalle telecamere sia effettivamente coinvolto nell'omicidio, ma anche dimostrare che Tizio, la cui immagine è compatibile all'80% con un individuo di cui è ignota l'identità, sia lo stesso soggetto. Infatti, lo strumento digitale di riconoscimento facciale si limita a consegnare un *output* che indica la similarità tra i tratti somatici rilevati e quelli presenti in un database di riferimento (Ignoto e Tizio sono compatibili all'80%, ma ciò non significa che l'identità di Ignoto e Tizio coincidano univocamente) [143]. Il *match* necessita dunque di essere integrato e corroborato da ulteriori elementi di prova, per completare

---

conoscibile quando non sia più presente; pertanto, la rappresentazione è il modo con cui un fatto può essere reso conoscibile da altre persone. Il fatto può essere rappresentato con immagini, parole, gesti o suoni». P. TONINI-C. CONTI, *Il diritto delle prove penali*, cit., p. 46.

[142] Cfr. P. TONINI-C. CONTI, *Il diritto delle prove penali*, cit., p. 45 e 46.

[143] Cfr. il capitolo II, § 4.

il quadro probatorio e garantire una valutazione fondata su criteri di coerenza, convergenza e affidabilità complessiva [144].

Nella diversa ipotesi in cui il sistema di riconoscimento facciale registri l'esatto momento in cui il soggetto colpisce la vittima con un'arma, il risultato prodotto da tale tecnologia può essere inteso come una prova rappresentativa (debole) dell'identità dell'autore del reato perché direttamente riferita [145]. Infatti, diversamente dalle prove dichiarative tipiche che potrebbero avere ad oggetto l'azione criminosa, il riconoscimento facciale automatizzato scompone i vari elementi dell'accadimento, prendendo in considerazione soltanto il dato biometrico del volto, ricavabile dal soggetto agente. In questa prospettiva, il *match* costituisce appunto una prova rappresentativa, seppur debole, dell'identità di quest'ultimo, e un mero indizio rispetto al fatto principale, oggetto dell'imputazione.

Riassumendo, giova ribadire la necessità di distinguere concettualmente due piani differenti dell'analisi probatoria nel contesto del riconoscimento facciale automatizzato: da un lato, il contenuto fenomenologico delle videoregistrazioni, che documentano la presenza o il comportamento di un soggetto in un determinato contesto spazio-temporale; dall'altro, l'esito del processo algoritmico di comparazione biometrica, ossia il cosiddetto *match*, che rappresenta il risultato derivante dall'elaborazione di dati biometrici attraverso specifici modelli computazionali. Tale scissione concettuale appare indispensabile ai fini di una corretta qualificazione giuridica degli elementi acquisiti nel procedimento penale. Da un lato, la videoregistrazione, in quanto riproduzione audiovisiva diretta di una determinata porzione di realtà, è idonea a documentare in modo immediato e percepibile una pluralità di circostanze fattuali: dalla mera presenza di un soggetto in un'area geografica delimitata, alla concreta esecuzione di un'azione da parte dello stesso. Dall'altro, la percentuale di compatibilità generata da un sistema di riconoscimento facciale automatizzato è finalizzata a valutare il grado di somiglianza tra i dati biometrici del soggetto ignoto rilevato (ad esempio, da un fotogramma) e i profili precedentemente archiviati in una

---

[144] Cfr. M. TARUFFO, *La prova dei fatti giuridici. Nozioni generali*, Giuffrè, Milano, 1992, p. 198. Cfr. *ex multis*, Cass. pen., sez. I, 21 luglio 2020, n. 21823, *inedita*, ove la Corte sottolinea il valore meramente indiziario di un risultato di compatibilità restituito dal software di riconoscimento facciale SARI rispetto ai fatti oggetto di prova, evidenziando come in quel caso «le immagini poste alla base del riconoscimento non erano nitide e non consentivano di riconoscere le fattezze, l'abbigliamento e diversi particolari dell'accoltellatore, per cui non era sostenibile la sussistenza di elementi gravi».

[145] Cfr. P. TONINI-C. CONTI, *Il diritto delle prove penali*, cit., p. 45.

banca dati. Tale esito computazionale, pur direttamente riferibile all'identità del soggetto, non la dimostra in modo certo e univoco, ma ne esprime una verosimiglianza statistica, basata su parametri variabili quali la qualità dell'immagine, il *training set* dell'algoritmo e la struttura della popolazione di riferimento.

Questo vale per i sistemi impiegati *a posteriori* ma anche per quelli *in tempo reale*, in cui il *match* biometrico stabilito dal sistema restituisce un valore rappresentativo del grado di similarità fra il dato acquisito e quello conservato nella *watchlist*. Per questi motivi, l'*output* si configura sempre come una prova debole, rappresentativa di un fatto secondario – ossia la mera somiglianza tra le immagini del volto dell'aggressore ignoto e quello di un soggetto previamente identificato (Tizio) – che, solo se integrato entro un quadro probatorio più ampio e corroborato da ulteriori elementi, può potenzialmente concorrere alla dimostrazione del fatto principale e all'accertamento dell'identità dell'autore del delitto [146].

6.1. *L'attendibilità del* match *biometrico*

Sul piano dell'attendibilità della prova, come chiarito in precedenza, la percentuale di compatibilità fra i volti risulta influenzata da molteplici fattori, la cui interazione incide in modo significativo sulla robustezza epistemologica del risultato ottenuto. Si ricorda come, tra questi rientrano per esempio la qualità del dato biometrico, la configurazione algoritmica del software e il tasso di errore del sistema [147].

Si è anche già evidenziato che caratteristiche come il DNA o le impronte digitali, basate su informazioni biologiche permanenti e altamente distintive, offrono un elevato grado di "riferibilità individualizzante" [148]. Al contrario, tratti biometrici come le impronte facciali, soggette a variabili ambientali (luce, angolazione, modalità dell'acquisizione), risultano meno affidabili.

---

[146] Su questo punto cfr. M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, cit., p. 17; S. QUATTROCOLO, *L'ammissione della prova alla luce della rivoluzione digitale*, in E.M. CATALANO, P. FERRUA (a cura di), *Corderiana*, Giappichelli, Torino, 2023, p. 181 ss.; P. SEVERINO, *Intelligenza artificiale e diritto penale*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020, p. 544.

[147] Cfr. il capitolo II, § 4.6.

[148] *Ibidem*.

L'intrinseca instabilità del dato comporta una maggiore esposizione a falsi positivi e negativi, riducendo l'attendibilità del riconoscimento facciale rispetto a tecnologie biometriche tradizionalmente più stabili.

Un ulteriore profilo di criticità emerge analizzando la configurazione algoritmica del software utilizzato per il riconoscimento facciale. L'assenza di una soglia predefinita e standard di somiglianza oltre la quale il risultato di una comparazione possa essere considerato attendibile rappresenta un limite significativo. Questa lacuna si traduce in una fragilità strutturale del processo di identificazione automatizzata, poiché priva il risultato di un parametro tecnico condiviso, che possa fungere da criterio nella scelta tra un *match* attendibile e un risultato potenzialmente fallace. Nella maggior parte dei sistemi attualmente in uso, la misura della soglia di riconoscimento viene definita in modo arbitrario, spesso modulata in base alle esigenze operative o alle preferenze del gestore del sistema, senza che vi sia una validazione scientifica univoca o una normativa di settore che ne regoli l'impostazione in modo rigoroso.

Non può infine essere trascurato il fatto che i risultati ottenuti da tali strumenti derivino da *patterns* di confronto basati su modelli matematici complessi, i quali, pur essendo il frutto di tecnologie sofisticate, restano inevitabilmente soggetti a margini di errore [149]. Tali limiti non dipendono unicamente dalla qualità del modello di intelligenza artificiale, ma sono anche fortemente influenzati da fattori esogeni che possono compromettere la precisione del confronto.

Pertanto, l'affidabilità del *match* di riconoscimento facciale manifesta una debolezza strutturale che non può essere trascurata nel contesto della valutazione del giudice. Tale fragilità epistemologica è accentuata dalla natura meramente statistica del dato algoritmico, il quale, pur offrendo una misura di similarità tra due insiemi di caratteristiche biometriche, non esaurisce il processo analitico necessario per attribuire al risultato un significato probatorio coerente con le esigenze del contesto giudiziario.

Questo limite intrinseco può tuttavia essere mitigato attraverso un'operazione di verifica critica condotta da un operatore esperto, il cui intervento si configura come un passaggio imprescindibile per la trasformazione del dato numerico in un'informazione giuridicamente significativa [150]. Nella scienza forense, "interpretare" un risultato fornito da un

---

[149] *Ibidem*.

[150] Cfr. R.J.F. YPMA-D. RAMOS-D. MEUWLY, *AI-based Forensic Evaluation in Court: The*

sistema automatizzato implica un processo cognitivo complesso, volto a trasformare l'*output* algoritmico – frutto di calcoli basati su modelli di riconoscimento prevalentemente statistici – in un'informazione dotata di valore probatorio specifico.

L'attività interpretativa si sostanzia, pertanto, nell'attribuzione di un significato giuridicamente rilevante al dato numerico rappresentato dalla percentuale di compatibilità, espressa come esito del processo algoritmico di comparazione. Tale operazione ermeneutica implica una valutazione contestualizzata che non può prescindere dalla riconduzione del dato tecnico al caso concreto, mediante un'analisi articolata e multidimensionale, in grado di integrare variabili extratecniche [151]. In particolare, la calibrazione del valore informativo della percentuale di similarità deve avvenire alla luce di una serie di elementi circostanziali e fattuali che possono incidere sensibilmente sull'affidabilità del risultato. In tale prospettiva, l'interpretazione del dato numerico non si riduce a una mera lettura meccanica del valore percentuale, ma si configura come un'operazione valutativa complessa, in cui le competenze tecniche devono coniugarsi con un'adeguata sensibilità giuridica, al fine di evitare l'attribuzione acritica di un peso probatorio eccessivo a un risultato che, per sua natura, costituisce un indice di somiglianza, suscettibile di ulteriori verifiche e raffronti.

Un parallelismo potrebbe essere tracciato tra questa attività e il lavoro svolto durante la fase di redazione dei brogliacci e di rielaborazione del captato nella disciplina delle intercettazioni. In talune circostanze, tale attività viene svolta da personale specializzato, dotato di competenze specifiche nell'ambito dell'ascolto investigativo [152]. Come noto, in presenza di difficoltà

Desiderability of Explanation and the Necessity of Validation, in Z. GERADTS-K. FRANKE (eds.), *Artificial Intelligence (AI) in Forensic Science*, John Wiley & Sons Inc, Hoboken, 2023, p. 6 ss.

[151] Cfr. *Best Practice Manual for Facial Image Comparison*, pubblicate dall'ENFSI-BPM-DI-01 Version, 01 – January 2018, reperibili su https://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf., ENFSI, *Best Practice Manual for Facial Image Comparison*, 2018, reperibile su https://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf. Sul tema v. D. MEUWLY-D. RAMOS-R. HARAKSIM, *A guideline for the validation of likelihood ratio methods used for forensic evidence evaluation*, in *Forensic Science International*, 276, 2017, p. 142-153.

[152] Per un generale approfondimento sul tema, *ex multis* cfr. G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, Giuffrè, Milano, 1987; F. CAPRIOLI, *Intercettazione e registrazione di colloqui tra persone presenti nel passaggio dal vecchio al nuovo codice di procedura penale*, in *Riv. it. dir. e proc. pen.*, 1991; A. CAMON, *Le intercettazioni nel processo penale*, Giuffrè, Milano, 1996; L. FILIPPI, voce *Intercettazioni telefoniche (diritto processuale penale)*

legate alla qualità del segnale, alla complessità linguistica o all'utilizzo di dialetti e gerghi particolari, l'autorità giudiziaria può disporre il ricorso a esperti in linguistica forense e fonetica applicata, i quali si occupano non solo della mera trasposizione grafica del parlato, ma anche dell'interpretazione di elementi prosodici, paralinguistici e contestuali che possono influire sul significato degli enunciati [153]. La trascrizione del captato si configura dunque come un'operazione altamente delicata, in cui la fedeltà e l'accuratezza della trasposizione dipendono da una serie di variabili acustiche e linguistiche. La maggior parte delle problematiche che possono sorgere in questo tipo di attività derivano dal rumore in sottofondo, dalla sovrapposizione di voci, dalla qualità delle registrazioni e dalla presenza di espressioni idiomatiche o allusive. In questo contesto, l'attività dell'operatore specializzato assume un ruolo fondamentale, soprattutto quando le comunicazioni intercettate avvengono con varietà linguistiche regionali o in forme di linguaggio criptato. Il dialettologo o il linguista forense analizzano le caratteristiche fonetiche, morfosintattiche e lessicali del parlato, considerando il contesto sociolinguistico di riferimento per interpretare correttamente le sfumature semantiche che potrebbero sfuggire a un orecchio non esperto. Anche in questo caso, dunque, l'obiettivo è quello di valutare l'accuratezza e la robustezza di un risultato restituito da una macchina, basandosi su metodologie scientificamente fondate.

6.1.1. *Il ruolo del calcolo del rapporto di verosimiglianza*

Come si ricorderà, nell'*iter* di attribuzione di significato al *match* biometrico, un ruolo centrale è rivestito dal calcolo del cosiddetto "rapporto di verosimiglianza" (cd. *likelihood ratio*), il quale rappresenta l'espressione quantitativa del valore probatorio di una percentuale di compatibilità

in *Enc. dir.*, Agg, VI, Milano, 2002, p. 565; G. VISONE, *Le intercettazioni tra perizia trascrittiva e prova testimoniale*, in *Proc. pen. e giust.*, 5, 2018; D. SCARPINO, *La disciplina delle intercettazioni telefoniche ed ambientali*, in *Riv. pen. dir. e proc.*, 2023.

[153] Per un approfondimento cfr. V. GALATÀ, *Aspetti tecnici sulle intercettazioni: analisi dei segnali e dei supporti*, in L. ROMITO (a cura di), *Manuale di Linguistica forense. Dalle lezioni del Corso sperimentale in "Perito-fonico-trascrittore forense" realizzato dall'I.RI.FO.R e dall'UniCal*, Bulzoni, Roma, 2013, p. 123-172, L. ROMITO-V. GALATÀ, *Speaker Recognition in Italy: evaluation of methods used in forensic cases*, in *Language Design*, 1, 2008, p. 229-240; L. ROMITO-M. MADDALON-J. TRUMPER, *Atteggiamento della Magistratura nei confronti delle perizie foniche. Il paradigma scientifico: unico o molteplice?*, *Atti del convegno VI Giornate di Studio del Gruppo di Fonetica Sperimentale (G.F.S.) 23*, Fondazione Ugo Bordoni, Roma, 1996, p. 34-45.

biometrica [154]. Questo calcolo matematico-statistico consente di "contestualizzare" il *match* prodotto dal sistema automatizzato, offrendo un'indicazione quantitativa della coincidenza fra le varie identità confrontate, ma non esaurisce ancora il processo valutativo, che richiede comunque una verifica da parte dell'esperto [155]. Tale operazione di verifica non costituisce un mero controllo formale, bensì rappresenta un momento di validazione scientifica del dato, finalizzato a garantire che il risultato non sia il prodotto di errori sistemici, *bias* algoritmici o anomalie tecniche. L'esperto forense, infatti, non si limita a confermare o smentire il *match* proposto dal sistema, ma applica metodologie di analisi conformi agli standard internazionali e alle procedure validate dalla comunità scientifica di riferimento [156]. Questo approccio metodologico consente di integrare il calcolo algoritmico con la capacità interpretativa dell'analista, riducendo il rischio di attribuzioni errate e aumentando la robustezza epistemologica del risultato.

Sul piano giuridico, la verifica del risultato da parte dell'operatore e il calcolo del rapporto di verosimiglianza rappresentano presidi indispensabili per garantire la conformità dell'attività di riconoscimento facciale ai principi fondamentali in materia di protezione dei dati personali e di tutela dei diritti fondamentali dell'individuo [157].

Inoltre, tale conclusione ben si inserisce nel quadro tracciato dagli artt. 22 GDPR, 11 LED, 8 d.lgs. n. 51/2018 – che pongono il divieto di decisioni basate esclusivamente su un trattamento automatizzato dei dati personali produttivo di effetti giuridici negativi in assenza di un intervento umano nel processo decisionale [158]. In questo scenario si può cogliere una eco del

---

[154] Cfr. il capitolo II, § 4.4.

[155] Cfr. R.J.F. YPMA-D. RAMOS-D. MEUWLY, *AI-based Forensic Evaluation in Court: The Desiderability of Explanation and the Necessity of Validation*, cit., p. 6; G. TESSITORE, *Riconoscimento automatico del volto e confronto in ambito forense*, in P. DI SIMONE-A. MANGIARACINA-L. PARLATO (a cura di), *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, Palermo University Press, Palermo, 2023, p. 66; EUROPEAN NETWORK OF FORENSIC SCIENCE INSTITUTES, *Guideline for Facial Recognition System End Users*, ENFSI-DI-GDL-001, Version 001 – November 2022; EUROPEAN NETWORK OF FORENSIC SCIENCE INSTITUTES, *Best Practice Manual for Facial Image Comparison*, ENFSI-BPM-DI-01, 2018; FACIAL IDENTIFICATION SCIENTIFIC WORKING GROUP, *Minimum Guidelines for Facial Image Comparison Documentation*, 2020.

[156] Cfr. G. TESSITORE, *Riconoscimento automatico del volto e confronto in ambito forense*, cit., p. 81.

[157] Cfr. il capitolo III, § 4.

[158] Cfr. il capitolo III, § 4.1. È prevista una deroga qualora «sia autorizzata dal diritto

criterio della "prova unica e determinante", elaborato nell'ambito della giurisprudenza della Corte di Strasburgo con riferimento al caso in cui una persona che abbia reso dichiarazioni al pubblico ministero o alla polizia nel corso delle indagini, non si presenti in dibattimento per sottoporsi all'esame testimoniale [159]. Secondo la Corte [160], una prova siffatta deve essere sottoposta a rigorosi criteri di scrutinio, al fine di assicurare il rispetto delle garanzie sancite dall'art. 6 della Convenzione. Svolgono questa funzione, per esempio, la presenza di riscontri [161], adeguate *directions* alla giuria [162], un'analitica motivazione [163], l'acquisizione della videoregistrazione del colloquio [164], oppure il fatto che le dichiarazioni in questione siano state rese davanti a un giudice, o che, comunque, nel contesto della loro

dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento». Il par. 2 esclude che il trattamento possa basarsi su una categoria particolare di dati personali, tra cui i dati biometrici, «a meno che non siano in vigore misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato». L'art. 5 par. 3, AI Act specifica che «nessuna decisione che produca effetti giuridici negativi su una persona può essere presa unicamente sulla base dell'*output* del sistema di identificazione biometrica remota "in tempo reale"».

[159] Per una ricostruzione sul tema A. CABIALE, *I limiti alla prova nella procedura penale europea*, Wolters Kluwer Cedam, Milano, 2019, p. 112 ss.; M. AURIEMMA, *Sulla prova "unica o determinante". Il caso Al Khawaja e Tahery c. Regno Unito*, in *Arch. pen.*, 2012, p. 598-600; R. CASIRAGHI, *Testimoni assenti: la Grande camera ridefinisce la regola della 'prova unica o determinante'*, in *Cass. pen.*, 2012, p. 3116; I.H. DENNIS, *AlKhawaja and Tahery v United Kingdom, Commentary*, in *Criminal Law review*, 2012, p. 376-378; più risalenti, M. DANIELE, *Principi costituzionali italiani e ingerenze europee in tema di prova dichiarativa*, in *Riv. it. dir. proc. pen.*, 2011, p. 1008; E.N. La ROCCA, voce *Prova (prospettive europee)*, in *Dig. disc. pen.*, Agg. IV, Torino, 2008, p. 844-847; M. MONTAGNA, *Dichiarazioni irripetibili ed irreperibilità del teste*, in *Arch. pen.*, 2011, p. 664-665; A. PAGLIANO, *Le discrasie del sistema processuale penale italiano in tema di letture e contestazioni*, in *Dir. pen. e proc.*, 2011, p. 1531; A. BALSAMO, *La Corte di Strasburgo e i testimoni assenti: gli sviluppi del 'nuovo corso' avviato dalla sentenza Al-Khawja, C. eur. diritti uomo, Sez. III, 19/2/2013, n. 61800/08, Gani c. Spagna*, in *Cass. pen.*, 2013, p. 2840.

[160] C. eur., Grande Camera, 15 dicembre 2011, *Al-Khawaja e Tahery c. Regno Unito*, § 18 e C. eur., Grande Camera, 15 dicembre 2015, *Schatschaschwili c. Germania*, § 109, C. eur., *Seton c. Regno Unito*, 31 marzo 2016, rich. nn. 55287/2010.

[161] Cfr. C. eur. 9 luglio 2013, *Sică c. Romania*, § 76; C. eur. 19 giugno 2012, *Hümmer c. Germania*, §§ 49-50; C. eur. 6 dicembre 2012, *Pesukic c. Svizzera*, § 48.

[162] C. eur., Grande Camera, 15.12.2011, *Al-Khawaja e Tahery c. Regno Unito*, § 157.

[163] C. eur. 9 luglio 2013, *Bobeş c. Romania*, § 46.

[164] C. eur., Grande Camera, 15 dicembre 2015, *Schatschaschwili c. Germania*, § 127.

assunzione, la difesa abbia potuto interagire anche indirettamente con il dichiarante [165].

In questo parallelismo, la supervisione umana costituisce il fattore idoneo a evitare che decisioni già potenzialmente lesive dei diritti fondamentali siano affidate in modo esclusivo a sistemi automatizzati, i quali, per quanto avanzati, possono essere affetti da distorsioni statistiche o limitazioni tecniche. In questa prospettiva, il calcolo del rapporto di verosimiglianza da parte dell'operatore svolge una funzione di mediazione epistemologica, necessaria per garantire non solo che l'evidenza biometrica sia correttamente interpretata e contestualizzata, ma anche come presidio metodologico contro il rischio di automatismi cognitivi indotti dal sistema algoritmico [166].

Ovviamente, risulta fondamentale porre il tecnico nella condizione di «comprendere il sistema di riconoscimento facciale e i suoi limiti, nonché di interpretarne correttamente i risultati», predisponendo «un ambiente di lavoro e un'organizzazione tali da controbilanciare gli effetti della distorsione dell'automazione, evitando di favorire l'accettazione acritica dei risultati» [167].

In conclusione, lo scenario ricostruito nei passaggi che precedono, delinea un duplice meccanismo di garanzia contro i rischi di un impiego disinvolto dei risultati del riconoscimento facciale per finalità probatorie. Non solo, infatti, le caratteristiche tecniche e i capisaldi della scienza biometrica stabiliscono dei fattori di esclusione della idoneità di tali risultati a provare l'identificazione tra due volti. Laddove tuttavia tale dato dovesse superare lo sbarramento ammissivo – poiché nel caso concreto ritenuto idoneo a provare fatti di cui all'art. 187 c.p.p. – l'insieme delle fonti e delle interpretazioni interne ed europee, formali e/o giurisprudenziali – che

---

[165] C. eur., Grande Camera, 15. dicembre 2015, *Schatschaschwili c. Germania*, § 157.

[166] Per questa ragione, l'art. 14 par. 5 dell'AI Act prevede che gli *output* dei sistemi di identificazione biometrica da remoto possano essere utilizzati per decisioni operative solo previa verifica indipendente da parte di due esperti qualificati. Questa misura risponde alla necessità di mitigare i rischi connessi all'assenza del coinvolgimento diretto del soggetto interessato nella raccolta dei dati biometrici, circostanza che incrementa la probabilità di errori nell'identificazione, considerato che i dati vengono acquisiti in modo indiretto e senza interazione diretta. Tuttavia, se l'impiego avviene «a fini di contrasto, migrazione, controllo delle frontiere o asilo», la normativa può esentare da tale obbligo se ritenuto sproporzionato rispetto agli scopi perseguiti. Cfr. il capitolo III, § 4.1.

[167] Cfr. EDPB, *Linee guida 05/2022 sull'uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto*, p. 23. Sul tema v. G. UBERTIS,*Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Dir. pen. cont.*, 4/2020, p. 83 ss.

vietano una decisione basata soltanto su un trattamento automatizzato, rappresenta l'estremo presidio a tutela della funzione cognitiva del processo.

Inoltre, è opportuno sottolineare che il regolamento sull'intelligenza artificiale muove un ulteriore passo in avanti quando prevede che qualsiasi persona interessata da una decisione adottata dal *deployer*, sulla base di un sistema di IA, vanti la pretesa a una spiegazione minima e comprensibile [168]. Questa, pur articolandosi in modo diverso a seconda del ruolo assunto dall'intelligenza artificiale nella procedura decisionale, si risolverà in «spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata» [169].

Da ciò discende, nella nostra prospettiva, un terzo presidio. Infatti, con riferimento ai provvedimenti giudiziari che si fondano, anche parzialmente, su un esito, pur valutato e calibrato dall'uomo, derivante da sistemi automatizzati di riconoscimento facciale, si potrebbe prefigurare l'obbligo di una motivazione rafforzata [170]. Ciò risponderebbe all'esigenza di garantire la trasparenza epistemologica del processo decisionale compiuto dal giudice, imponendo un controllo critico non solo sull'esito fornito dal sistema, verificato e ponderato dagli esperti, ma anche sui presupposti metodologici sottesi alla procedura di identificazione seguita. In tale prospettiva, il giudice dovrebbe esplicitare in modo rigoroso le ragioni per cui ritiene che il sistema soddisfi i requisiti di affidabilità propri della prova scientifica, anche alla luce

---

[168] Cfr. l'articolo 86, par. 1, AI Act. Si veda più ampiamente il capitolo III, § 4.1.

[169] Riguardo a quanto previsto dall'art. 3, par. 3 AI Act, le *Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*, p. 118 hanno chiarito che «*the procedures should provide instructions on the deployment of the RBI system, clarify the role of a human agent in verifying and interpreting the output and provide training to operate the system. The person in charge of human oversight should have sufficient 'AI literacy, training and authority' to understand how the system functions and when it underperforms or malfunctions*». Si rinvia a M.E. KAMINSKI-G. MALGIERI, *The Right to Explanation in the AI Act*, in *U of Colorado Law Legal Studies Research Paper*, No. 25-9, 2025.

[170] Sul tema della motivazione rafforzata cfr. M. CECCHI, *La motivazione rafforzata del provvedimento: un nuovo modello logico-argomentativo di stilus curiae*, Wolters Kluwer Cedam, Milano, 2021; M. CECCHI, *La "motivazione rafforzata" del provvedimento ovvero la "forza persuasiva superiore"*, in *Dir. pen. e proc.*, 2019, p. 1123 ss.; C. CONTI, *Sicurezza e riservatezza*, in *Dir. pen. e proc.*, 2019, 11, p. 1572 e M. CECCHI, *Il giudice dinanzi alla prova scientifica*, in *Arch. pen.*, 1, 2022, p. 11.

delle note criticità legate alla natura potenzialmente opaca (c.d. *black box*) dei *tools* di intelligenza artificiale [171].

Parallelamente, va considerata un'ulteriore ipotesi speculare: quella in cui il giudice, pur a fronte di un risultato tecnico "qualificato" da una determinata attendibilità, a seguito di una verifica di un operatore esperto, decida di non valorizzarlo nella sua decisione. In tal caso, non si tratterebbe di contraddire il principio del libero convincimento, ma piuttosto di declinare in forma rafforzata l'obbligo motivazionale, laddove vi siano elementi tecnici dotati di oggettività e suscettibili di controllo. Anche il mancato utilizzo di un *match* biometrico meritevole di considerazione esigerebbe dunque una motivazione analitica, fondata su una valutazione ragionata sulla sua irrilevanza, inattendibilità o insufficienza, con l'obiettivo di evitare che la decisione giudiziaria si sottragga ad ogni scrutinio critico in presenza di elementi potenzialmente significativi.

In altre parole, il giudice dovrebbe motivare la propria decisione dimostrando di aver effettuato un vaglio critico sulla "scientificità" dello strumento [172]. Tale adempimento comporterebbe, quindi, un duplice livello di scrutinio: da un lato, sull'affidabilità tecnica del sistema utilizzato e della successiva verifica da parte dell'operatore; dall'altro, sulla coerenza logico-giuridica del percorso argomentativo che ha condotto il giudice a integrare o meno tale evidenza nel proprio giudizio. Se è vero che tale onere argomentativo potrebbe rappresentare un aggravio per l'attività giudiziale, è altrettanto vero che esso sarebbe ampiamente compensato dal miglioramento della qualità e dell'affidabilità delle decisioni [173].

---

[171] Cfr. G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Dir. pen. cont.*, 4/2020, p. 78 ss.

[172] Cfr. Cass. pen., sez. I, 12 ottobre 2018, n. 52872, in *CED Cass.*, n. 275058.

[173] Cfr. V. MANES, *L'Oracolo algoritmico e la giustizia penale*, cit., p. 21.

Capitolo VI
Riflessioni e prospettive *de iure condendo*

SOMMARIO: 1. Osservazioni conclusive. Da dove veniamo? Chi siamo? Dove andiamo? – 2. Gli standard tecnici comuni tra certezza del diritto e innovazione tecnologica. – 3. Le modalità *in tempo reale* e a posteriori entro il sistema codicistico in una prospettiva *de iure condendo*.

1. *Osservazioni conclusive. Da dove veniamo? Chi siamo? Dove andiamo?*

Al termine di questo percorso di analisi, è possibile confermare l'assoluta unicità che caratterizza le tecnologie di riconoscimento facciale rispetto a qualsiasi altro strumento computazionale attualmente in uso alle autorità di *law enforcement* [1]. Le peculiarità di questi sistemi si radicano nel fatto che il rischio di violazione dei diritti e delle libertà fondamentali risulta amplificato. Ciò avviene principalmente perché il trattamento dei dati personali ha luogo senza il coinvolgimento attivo del soggetto interessato, determinando una forma di sorveglianza passiva continuativa e tendenzialmente occulta. Al contempo, questa stessa caratteristica rappresenta un importante vantaggio operativo per le autorità, poiché consente l'acquisizione dei dati senza la necessità di procedure complesse o di un'interazione diretta con gli individui monitorati, ottimizzando così l'efficienza delle fasi di raccolta e di analisi delle informazioni.

Tuttavia, sul piano probatorio, i risultati di una comparazione automatizzata sono limitati dalla scarsa capacità dimostrativa della percentuale di similarità generata dai sistemi. Il *match* biometrico, se considerato isolatamente e privo di una valutazione critica da parte di un operatore, può solo

[1] Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021, p. 287.

costituire un elemento di prova (debole) dell'identità del soggetto e un mero indizio rispetto al fatto principale, oggetto dell'imputazione, anche qualora la ripresa video abbia documentato l'intero svolgimento del fatto di reato[2]. L'*output* generato rappresenta sempre e solo un indice della coincidenza tra l'identità ignota e i profili registrati nella banca dati di riferimento con cui è stata rilevata una corrispondenza calcolata in percentuale.

Nonostante la sua circoscritta capacità dimostrativa e i limiti tecnici descritti, però, la tecnologia di riconoscimento facciale si configura come un efficace strumento per agevolare alcuni processi di consultazione precedentemente eseguiti in via analogica, consentendo così un incremento significativo dell'efficienza durante le attività di identificazione.

Inoltre, il costante progresso nei settori di applicazione dell'intelligenza artificiale e dell'elaborazione delle immagini lascia presupporre che, nel prossimo futuro, i sistemi di riconoscimento biometrico saranno in grado di eseguire comparazioni tra volti con un livello di accuratezza e affidabilità sempre più elevato. I continui avanzamenti delle tecniche di apprendimento profondo (cd. *deep learning*), l'incremento delle capacità computazionali e l'ottimizzazione dei modelli di analisi biometrica potrebbero contribuire a una riduzione delle attuali criticità.

In tale contesto, dunque, la riflessione scientifica non può più incentrarsi sulla possibilità di un divieto generalizzato e assoluto dell'impiego delle tecnologie di riconoscimento facciale, posizione che risulterebbe ormai anacronistica, disancorata dalle dinamiche reali del progresso tecnologico e dalle concrete esigenze operative degli apparati di *law enforcement.* Una simile impostazione di carattere meramente interdittivo rischierebbe infatti di rimanere priva di efficacia pratica, oltreché inadeguata ad affrontare le sfide poste dall'implementazione ormai diffusa di tali strumenti, i cui effetti incidono in modo significativo sul tessuto sociale e giuridico contemporaneo.

Piuttosto, la comunità scientifica e il legislatore sono oggi chiamati a compiere uno sforzo ermeneutico e sistematico volto all'attuazione di un quadro regolatorio compiuto ed equilibrato, capace di bilanciare in modo ragionevole l'efficienza investigativa con la salvaguardia dei diritti fondamentali dell'individuo. Il centro del dibattito deve spostarsi verso l'attuazione a livello nazionale di un sistema normativo strutturato e dinamico, che sia in grado di regolare l'impiego delle tecnologie biometriche in modo proporzionato, trasparente e sottoposto a controlli effettivi onde evitare derive

[2] Cfr. il capitolo V, § 5.

autoritarie o indebite compressioni delle libertà costituzionalmente garantite.

In questo scenario, il tema della trasparenza tecnica diventa cruciale. L'implementazione della normativa europea sull'intelligenza artificiale presuppone, in via preliminare, l'adozione di meccanismi di accesso e divulgazione che garantiscano un'adeguata conoscenza delle cifre tecniche di tali strumenti da parte dei soggetti coinvolti e della collettività. Un'efficace strategia di trasparenza istituzionale dovrebbe includere la pubblicazione di dati aggiornati sui tassi di errore, con particolare attenzione alla frequenza dei falsi positivi e falsi negativi, al fine di monitorare l'attendibilità e l'impatto concreto sull'incremento e sull'adozione di tali sistemi [3].

Allo stesso modo, l'accessibilità dovrebbe riguardare anche la frequenza di impiego delle tecnologie di riconoscimento facciale da parte delle autorità di *law enforcement*, elemento essenziale per prevenire derive di sorveglianza massiva e garantire un impiego proporzionato e giustificato rispetto agli obiettivi perseguiti. Un'adeguata regolamentazione dell'uso di tali strumenti richiede la pubblicazione di informazioni relative al numero di operatori autorizzati, in modo da assicurare un controllo rigoroso sui soggetti legittimati a impiegarli, evitando usi impropri o eccessivamente discrezionali. La trasparenza non è più solo un requisito tecnico ma diventa condizione imprescindibile per il controllo democratico di questa tecnologia.

Il quadro descritto sollecita altresì una riflessione critica sull'opportunità o meno di estendere gli ambiti applicativi dei sistemi di riconoscimento facciale come, del resto, sembrerebbero suggerire le recenti iniziative legislative a livello europeo e nazionale [4]. La regolamentazione, ancora in fase di attuazione, sembra infatti orientarsi verso una progressiva "normalizzazione" dell'uso di questa tecnologia in ambito securitario, in prospettiva di un ampliamento delle possibilità di ricorso a questi strumenti per le autorità di *law enforcement*. Questo approccio non può che essere

[3] Sul piano interno si segnala il rigetto da parte del Senato della Repubblica dell'emendamento al disegno di legge n. 1146 sull'intelligenza artificiale (cfr. il capitolo IV, § 3), che proponeva l'introduzione di un obbligo di trasparenza istituzionale in materia di identificazione biometrica. La proposta prevedeva, in particolare, la pubblicazione annuale di una relazione a cura del Garante per la protezione dei dati personali, volta a documentare l'impiego delle tecnologie di identificazione biometrica sul territorio nazionale. Cfr. L. CARRER, *Il Senato boccia l'istituzione di un'autorità indipendente per l'intelligenza artificiale*, in *editorialedomani.it*, 20 marzo 2025.

[4] Cfr. il capitolo IV.

accompagnato dall'implementazione di una disciplina normativa rigorosa che definisca con precisione i limiti di utilizzo in conformità alle garanzie procedurali. Sul piano nazionale, la questione si traduce di riflesso nel tentativo di elaborare una regolamentazione costituzionalmente orientata, in cui la ricerca, lo sviluppo e l'applicazione delle tecnologie di riconoscimento facciale siano improntate al rispetto dei principi fondamentali. L'impatto trasversale di tali sistemi sui diritti richiede un approccio normativo che non si limiti a una tutela settoriale, ma che consideri la complessità delle interazioni tra garanzie diverse ma interconnesse, come la libertà personale, la privacy, la protezione dei dati personali, la libertà di espressione e di manifestazione del pensiero, la libertà di riunione e il divieto di discriminazione.

V'è da dire che l'esigenza di porre solidi argini normativi contro gli abusi investigativi e l'uso sproporzionato di tecnologie invasive affonda le proprie radici in un dibattito giuridico di lungo corso, caratterizzato dalla necessità di coniugare il progresso scientifico con la tutela dei diritti fondamentali della persona. Come visto, la Corte costituzionale già con la pronuncia 238 del 1996, in tema di prelievi ematici coattivi, facendo leva sull'inviolabilità della libertà personale, ha delineato principi di portata generale che costituiscono ancora oggi il fondamento teorico per affrontare l'incessante incremento dell'impiego delle innovazioni scientifiche nel processo penale, il cui impatto si estende ben oltre la dimensione strettamente probatoria[5]. I recenti approdi scientifici permettono infatti di ricavare dai campioni biometrici dati predittivi sulla salute del soggetto, includendo informazioni relative a patologie in essere o potenziali, con implicazioni non solo per la persona direttamente coinvolta, ma anche per il suo patrimonio genetico familiare e per contesti sociali più estesi.

L'attuale assetto normativo che disciplina l'impiego delle tecnologie di riconoscimento facciale appare contrassegnato da evidenti profili di insufficienza sistemica, tanto nella struttura, quanto nei contenuti prescrittivi, i quali risultano ancor più inadeguati se posti a confronto con le più articolate e rigorose disposizioni normative che regolano strumenti di identificazione di natura differente, quali, *in primis*, l'analisi del DNA.

Il confronto tra le due discipline ha messo in luce le differenze sul piano delle garanzie e del rigore regolatorio non più giustificabili alla luce della crescente incidenza che le tecnologie di riconoscimento facciale esercitano

[5] Cfr. il capitolo III, § 2.

sulle sfere di libertà e sulla riservatezza dell'individuo [6]. Tale considerazione è valida anche se i due tratti biometrici presentano proprietà morfologiche, strutturali e funzionali profondamente differenti: l'analisi del DNA si fonda su caratteristiche biologiche uniche e irripetibili per ciascun individuo, la cui architettura genetica rimane invariata nel tempo, offrendo un elevato grado di affidabilità scientifica. Al contrario, il riconoscimento facciale si basa su tratti somatici che possono subire modificazioni fisiologiche e ambientali, risultando maggiormente suscettibile a errori, specialmente nei sistemi operativi *in tempo reale*.

Tuttavia, la presenza di analogie tra i due metodi di riconoscimento, pur nella consapevolezza delle divergenti caratteristiche tecniche e scientifiche che ne connotano il funzionamento, non può essere sottovalutata sul piano della disciplina giuridica. Entrambi, infatti, concorrono alla ricostruzione di profili identificativi, agendo in profondità sulla sfera giuridicamente protetta della libertà morale e della riservatezza individuale, configurandosi dunque come strumenti dotati di una rilevante forza intrusiva [7]. In tal senso, tanto l'impronta genetica quanto l'immagine facciale, tradotte in rappresentazioni digitalizzate e sottoposte a processi automatizzati, si prestano a impieghi potenzialmente idonei a ledere diritti fondamentali, se non sottoposti a rigorosi presìdi normativi.

In questa prospettiva, appare indispensabile valorizzare i principi sanciti dagli artt. 2, 13 Cost., 8 Conv. eur. uomo, 7 e 8 CDFUE che tutelano la libertà personale e il diritto alla riservatezza come diritti inviolabili [8], nel tentativo di elaborare casi tipici e modalità specifiche di ricorso alle tecnologie biometriche, idonee a vincolare l'attività degli organi di *law enforcement.* A fronte delle sfide poste dall'evoluzione tecnologica, è emersa l'urgenza di approntare una tutela rafforzata del cosiddetto "corpo elettronico", inteso come l'insieme delle informazioni digitali che costituiscono l'identità personale nell'era della società dell'informazione. La protezione effettiva di tale dimensione identitaria impone la predisposizione di limiti normativi chiari e stringenti che regolino l'utilizzo delle tecnologie di riconoscimento facciale e, più in generale, delle diverse tecnologie biometriche, al fine di prevenire derive incompatibili con il quadro costituzionale e sovranazionale

[6] Cfr. il capitolo III, §§ 2 e 4.

[7] *Ibidem*.

[8] Cfr. M. TORRE, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. e proc.*, 8, 2021; G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 343.

di riferimento. L'adozione di una normativa chiara e dettagliata, nonché la previsione di un sistema di autorizzazione preventiva per l'uso di tali strumenti da parte delle autorità pubbliche, ovvero l'implementazione di meccanismi di revisione *ex post*, costituirebbero le garanzie essenziali per evitare riconoscimenti erronei o forme di controllo sociale e assicurare così il rispetto effettivo della riserva di legge e di giurisdizione.

2. *Gli standard tecnici comuni tra certezza del diritto e innovazione tecnologica*

Nel delineare i casi e le modalità di impiego di questi strumenti, risulta imprescindibile assumere quale punto di riferimento normativo il regolamento sull'intelligenza artificiale[9]. L'introduzione di un quadro di norme condiviso consente di facilitare certamente il superamento dell'attuale stato di vuoto e frammentazione normativa sul piano nazionale, caratterizzato da una logica casistica e settoriale, in cui il ricorso a questi strumenti è disciplinato sulla base di singole finalità o specifiche esigenze di pubblica sicurezza. L'adozione di una disciplina avente portata generale si configura infatti come un elemento essenziale per evitare un'applicazione disomogenea e discontinua della normativa nei diversi ordinamenti nazionali, riducendo il rischio di obsolescenza precoce delle disposizioni e garantendo, al contempo, un equilibrio tra esigenze di regolamentazione e flessibilità applicativa[10]. Il regolamento, pur perseguendo tale obiettivo, presenta disposizioni che conferiscono agli Stati membri un ampio margine di discrezionalità. Questo approccio, se da un lato rappresenta uno strumento per garantire un maggiore grado di adattabilità alle specificità nazionali, dall'altro potrebbe tradursi in un'accresciuta disomogeneità tra gli Stati membri, con ripercussioni significative sulla certezza del diritto e sull'effettività delle garanzie di tutela dei diritti fondamentali.

A livello europeo, la sfida attuale è quindi quella di uniformare il più possibile le varie discipline nazionali, al fine di garantire un quadro normativo

---

[9] Cfr. il capitolo IV, § 3.2.

[10] Rilievi analoghi in S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2015, p. 789.

coerente e omogeneo che favorisca la cooperazione tra gli Stati membri. Il rischio altrimenti è che l'assenza di un coordinamento normativo efficace favorisca un'applicazione non uniforme delle tecnologie biometriche, generando disparità di trattamento e compromettendo l'agognato equilibrio tra l'esigenza di accertamento processuale e la tutela dei diritti fondamentali.

Sul piano nazionale, è possibile immaginare un modello normativo procedimentale articolato su due livelli. Il primo strato dovrebbe essere costituito da un quadro di norme applicabili trasversalmente ai diversi impieghi procedimentali della tecnologia, tenendo conto delle differenze e delle specificità di funzionamento delle diverse modalità applicative. Questo primo piano di norme dovrebbe riportare le condizioni giuridiche necessarie per garantire l'uso della tecnologia nel rispetto dei diritti fondamentali e delle garanzie processuali (richiesta di autorizzazione, casi di attivazione dello strumento, limiti temporali di acquisizione dei dati ecc.).

Il secondo livello, da adottare con uno o più atti normativi, dovrebbe contenere le disposizioni tecniche generali, valide per tutti i sistemi di riconoscimento facciale, con particolare attenzione agli standard adottati, alle modalità di conservazione e gestione dei dati biometrici e ai protocolli di *audit* e supervisione.

La funzione di questo secondo strato di norme non si esaurirebbe, però, nella mera definizione degli aspetti tecnici di dettaglio, ma avrebbe un ruolo essenziale nel garantire un adeguato livello di *adattabilità*, necessario per rispondere all'evoluzione tecnologica e alle diverse esigenze applicative. Infatti, la separazione tra disposizioni procedimentali e normativa tecnica permetterebbe di uniformarsi sistematicamente al costante progresso scientifico, senza dover intervenire con continue modifiche, assicurando un quadro normativo stabile e coerente nel tempo [11]. L'adeguamento progressivo della disciplina consentirebbe di superare la tradizionale rigidità delle norme, evitando che esse rischino di "nascere" già obsolete, a fronte dell'accelerazione dell'innovazione [12]. In questa prospettiva, la regolamentazione dovrebbe

---

[11] Cfr. U. PAGALLO, *Algo-Rhythms and the Beat of the Legal Drum*, in *Philos. Technol.*, 2018, 31, p. 520; R. KENNEDY, *Algorithms and the Rule of Law*, in *Computers and Law*, 2017, p. 23 ss.; A. IANNUZZI, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Editoriale scientifica, Napoli, 2018, p. 2; G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 334; A. TAEIHAGH, *Governance of artificial intelligence*, in *Policy and Society*, 2021, p. 9 ss.

[12] Cfr. U. PAGALLO, *Intelligenza Artificiale e diritto. Linee guida per un oculato intervento normativo*, in *Sist. intell.*, 3, 2017, p. 626 ss., che distingue tra "neutralità tecnologica della

dunque svilupparsi secondo una logica "incrementale", nella quale il costante aggancio temporale con l'evoluzione tecnica e giurisprudenziale permetterebbe di mantenere un equilibrio tra certezza del diritto e innovazione tecnologica.

Venendo ai passaggi normativi più specifici, l'architettura di questo secondo strato di regole dovrebbe aprirsi con la definizione di un glossario tecnico condiviso, che stabilisca in modo univoco i vari passaggi del processo di riconoscimento, dall'acquisizione all'elaborazione, dal confronto alla conservazione dei dati. Il riferimento a un elenco di definizioni comuni è essenziale per evitare ambiguità interpretative e per uniformare i protocolli operativi adottati per il funzionamento delle diverse modalità applicative del riconoscimento.

Riguardo alla prima fase di *acquisizione* del dato, indipendentemente dall'origine e dalla natura dell'immagine raccolta [13], sarebbe fondamentale garantire una risoluzione adeguata della rappresentazione dei tratti distintivi del volto e l'omogeneità delle condizioni di illuminazione [14]. Anche per la fase di *individuazione* o cd. *face detection*, si dovrebbe considerare un metodo comune alle due modalità operative, al fine di garantire un livello di robustezza elevato rispetto alla serie di fattori che possono influenzare la precisione della localizzazione, tra cui la variabilità delle espressioni facciali, l'orientamento del volto rispetto alla fotocamera, la presenza di occlusioni parziali e le condizioni di illuminazione [15].

Nei sistemi di riconoscimento *a posteriori*, in cui le immagini provengono anche da scansioni di fotografie analogiche, la fase di individuazione dei volti dovrebbe prevedere meccanismi di pre-elaborazione, tra cui la rimozione del rumore digitale, il miglioramento del contrasto e la correzione delle distorsioni geometriche. Nel caso di *dati generati automaticamente*, è essenziale che i modelli di individuazione siano in grado di distinguere tra volti

---

legge", in cui il legislatore non deve favorire una delle tecnologie per dare attuazione agli obiettivi prefissati, e "indifferenza tecnologica della legge", in cui le finalità perseguite dal legislatore non devono dipendere dalla tecnologia utilizzata.

[13] Si ricorda l'usuale distinzione fra i *dati trasformati/convertiti, ricavati* e *generati automaticamente*. Cfr. il capitolo II, § 5.

[14] Cfr. R.T. APTEKER-J.A. FISHER-V.S. KISIMOV-H. NEISHLOS, *Video acceptability and frame rate*, in *IEEE MultiMedia*, 2(3), 1995, p. 32-40; M.K. HASAN-M.S. AHSAN *et al.*, *Human Face Detection Techniques: A Comprehensive Review and Future Research Directions*, in *Electronics*, 10(19), 2021, p. 2354.

[15] Cfr. il capitolo II, § 4.6.

sintetici e reali, riducendo il rischio di falsi positivi che potrebbero alterare l'affidabilità del sistema di riconoscimento.

Segue poi la fase di *normalizzazione* dei volti acquisiti: un approccio normativo che imponga l'adozione di standard tecnici comuni per questa fase sarebbe indispensabile, non solo per migliorare la precisione dei processi di identificazione, ma anche per assicurare criteri di equità e imparzialità, minimizzando il rischio di discriminazioni algoritmiche derivanti da *bias* nei *dataset* impiegati [16].

Affinché il sistema possa operare con un elevato livello di accuratezza e robustezza, la popolazione dei database biometrici dovrebbe essere disciplinata attraverso rigorose disposizioni di selezione e validazione delle immagini archiviate. Anche a questi fini, gli operatori coinvolti dovrebbero acquisire una consapevolezza critica sulle potenzialità e sui limiti di tali strumenti. Non si tratta di richiedere competenze tecniche avanzate in ambito informatico, bensì di promuovere un approccio interdisciplinare che consenta al personale coinvolto di interfacciarsi in modo consapevole con i sistemi di intelligenza artificiale.

Con riferimento all'eventuale e successiva fase di *estrazione* dei *templates* biometrici, l'elaborazione del modello elettronico dovrebbe essere condotta con criteri che garantiscano l'uniformità dei dati rispetto a eventuali variazioni introdotte dal dispositivo di acquisizione o dalla modalità di digitalizzazione. Per tale ragione, affinché il sistema mantenga la compatibilità con standard internazionali, i *templates* considerati dovrebbero essere solo quelli conformi a formati interoperabili, garantendo così la possibilità di integrazione con database biometrici preesistenti.

Indipendentemente dalla modalità operativa integrata, si dovrebbero adottare criteri normativi uniformi per la conservazione esclusiva delle riprese e delle comparazioni che hanno prodotto un *match* positivo rispetto ai dati archiviati [17]. A questi fini, risulta fondamentale prestabilire una soglia condivisa di similarità cui fare riferimento. L'adozione di uno standard unico per tutti i sistemi garantirebbe coerenza operativa e ridurrebbe il rischio di disuguaglianze nell'interpretazione dei risultati di comparazione, facilitando l'interoperabilità tra piattaforme diverse e la conformità ai requisiti normativi. Solo i volti che superano la soglia di similarità predefinita potrebbero essere memorizzati e associati al relativo riferimento archivistico. Questa

[16] *Ibidem*.

[17] Cfr. *infra* il § 3.

procedura permetterebbe di limitare il volume di dati conservati, riducendo l'impatto in termini di spazio di archiviazione e migliorando la sicurezza complessiva del sistema.

La durata di conservazione dei dati, analogamente ai campioni biologici e ai profili del DNA [18], potrebbe essere vincolata agli esiti dell'*iter* giudiziario. Per esempio, nei casi in cui i procedimenti si concludano con una sentenza di condanna, la conservazione delle immagini digitalizzate, dei relativi *templates* e degli eventuali *matches* positivi potrebbe essere parametrata in funzione della tipologia o della gravità del reato, della durata della pena e di eventuali esigenze di sicurezza pubblica. Per i reati di particolare allarme sociale o per i soggetti ritenuti pericolosi socialmente, la conservazione dei dati negli archivi di riferimento potrebbe essere giustificata da esigenze di prevenzione e monitoraggio, sempre nel rispetto di un quadro normativo rigoroso che limiti l'accesso e l'uso di tali informazioni esclusivamente agli scopi previsti dalla legge. In questi casi, sarebbe necessario garantire un meccanismo di revisione periodica della necessità di conservazione, evitando l'archiviazione indefinita dei dati, con un controllo giurisdizionale o amministrativo che ne valuti la persistenza dell'interesse pubblico alla loro disponibilità.

Viceversa, qualora il procedimento si concluda con una sentenza irrevocabile di proscioglimento, ovvero una sentenza di non luogo a procedere o un provvedimento di archiviazione, dovrebbe prevedersi un meccanismo di cancellazione sistematica dei dati collezionati. L'eliminazione dei dati potrebbe essere eseguita attraverso procedure automatizzate supervisionate e verificabili, in modo da garantire che nessuna traccia biometrica rimanga nei sistemi di archiviazione, riducendo al minimo il rischio di riutilizzo o recupero accidentale delle informazioni cancellate.

3. *Le modalità* in tempo reale *e* a posteriori *entro il sistema codicistico in una prospettiva* de iure condendo

Il primo livello di disposizioni normative, destinato a regolare in modo più puntuale l'applicazione del riconoscimento facciale nel procedimento

[18] Cfr. artt. 24 ss. d.P.R. n. 87/2016.

penale, dovrebbe invece essere calibrato sulle specificità operative degli strumenti impiegati, tenendo conto delle diverse esigenze che emergono nei vari contesti applicativi e delle implicazioni pratiche che derivano dal loro utilizzo. Un'impostazione normativa di questo tipo richiede dunque un approccio differenziato per le due modalità, *in tempo reale* e *a posteriori*, che tenga conto primariamente del funzionamento degli strumenti. La prima, come visto, intesa come attività a sorpresa, tendenzialmente occulta e continuativa, potenzialmente in grado di registrare e conservare i dati di tutti i soggetti esposti allo strumento. La seconda modalità, invece, predisposta per trattare e comparare il dato considerato con tutti quelli presenti nella banca dati di riferimento.

Partendo dai sistemi di riconoscimento facciale *in tempo reale*, il quadro normativo adottato a livello europeo presenta un grado di tutela rafforzato rispetto a quello previsto per gli strumenti *a posteriori*[19]. La motivazione di questa distinzione risiederebbe nella configurazione stessa della modalità applicativa, la quale, per sua natura, è potenzialmente in grado di elaborare e analizzare i dati biometrici di tutti i soggetti ripresi dalle telecamere, al fine di individuare eventuali corrispondenze con le informazioni già presenti in una *watchlist.* Questo meccanismo implica che la tecnologia sia in grado di trattare indiscriminatamente le immagini di un numero indefinito di individui, includendo anche coloro che non sono destinatari di alcun provvedimento investigativo o giudiziario.

Diversamente, i sistemi di riconoscimento facciale *a posteriori* operano secondo una logica più selettiva, per quanto a maglie larghe[20], effettuando il confronto tra immagini precedentemente acquisite e i dati biometrici di soggetti già identificati, in quanto fermati o fotosegnalati. In tale scenario, il trattamento biometrico è circoscritto a un database, per quanto certamente ampio, chiuso e predefinito, composto esclusivamente da individui che sono stati fermati o identificati per finalità di *law enforcement.*

L'adozione di una configurazione tecnica che consenta di registrare e conservare esclusivamente i dati biometrici dei soggetti individuati come compatibili con quelli già archiviati, previa verifica del superamento di una soglia prestabilita di similarità, potrebbe ridurre significativamente le differenze tra i due strumenti *in tempo reale* e *a posteriori*, sul piano della loro conformità ad alcuni principi fondamentali dell'ordinamento. La capacità di

[19] Cfr. il capitolo IV, § 3.2.2.

[20] Cfr. il capitolo II, § 4.2.

elaborare, filtrare e selezionare esclusivamente i dati biometrici di interesse, in entrambe le modalità operative, renderebbe il processo di riconoscimento non intrinsecamente più lesivo in un caso rispetto all'altro[21]. In questo modo, qualora la tecnologia fosse progettata per eliminare istantaneamente le immagini di tutti i soggetti non corrispondenti ai profili presenti nelle *watchlist*, si potrebbe realizzare una significativa assimilazione tra le due modalità di riconoscimento facciale, riducendo l'impatto della ricognizione indiscriminata eseguita dalla modalità *in tempo reale* sui diritti fondamentali. Se i volti delle persone non corrispondenti non fossero mai archiviati, né sottoposti a un trattamento, l'operazione di identificazione biometrica si limiterebbe a un mero confronto istantaneo tra l'immagine acquisita e il database esistente, eliminando ogni ulteriore forma di sorveglianza generalizzata. Questo meccanismo avvicinerebbe il riconoscimento facciale *in tempo reale* al modello *a posteriori*, poiché il trattamento biometrico sarebbe più circoscritto e non comporterebbe un'estensione massiva del controllo su individui estranei, sia sul piano della prevenzione, sia per eventuali procedimenti in corso.

Siffatta impostazione operativa, oltre a rappresentare un'evoluzione tecnologica già sperimentata in alcuni contesti[22], assicurerebbe una maggiore conformità ai principi di necessità, proporzionalità e minimizzazione dei dati, oltre a ridimensionare l'impatto negativo del *chilling effect* sulla libertà di autodeterminazione[23].

Tale previsione tecnica potrebbe dunque contribuire al superamento della tradizionale distinzione normativa tra riconoscimento facciale *in tempo reale* e *a posteriori.* In questo modo, sul piano normativo, si potrebbe in primo luogo annoverare il ricorso ai sistemi di riconoscimento facciale fra le diverse attività compiute dalla polizia giudiziaria durante la fase delle indagini per finalità meramente identificative. Il riconoscimento facciale, in entrambe le modalità applicative, potrebbe costituire uno strumento di ausilio per l'accertamento dell'identità di soggetti fermati o sottoposti a controlli di sicurezza, con la possibilità di attivare il sistema esclusivamente quando le procedure ordinarie di identificazione risultino inadeguate. Il ricorso al riconoscimento facciale in tale contesto dovrebbe essere inteso come *extrema*

---

[21] Cfr. F. PAOLUCCI, *From Global Standards to Local Safeguards: The AI Act, Biometrics, and Fundamental Rights*, in *SSRN*, 2024.

[22] Cfr. il capitolo III, § 4.3.

[23] Cfr. il capitolo III, § 1.

ratio, ovvero come strumento residuale, attivabile solo nel caso in cui l'identificazione mediante metodi tradizionali si riveli oggettivamente impraticabile e sempre nel rispetto del principio di proporzionalità, che impone di adottare il mezzo meno invasivo necessario al raggiungimento dello scopo preposto. Rimane sempre fermo che l'impiego dei due strumenti dovrebbe essere rigidamente circoscritto alle finalità specifiche di identificazione, senza estendersi a ipotesi non contemplate dal quadro normativo di riferimento, evitando così un'applicazione arbitraria o sproporzionata della tecnologia per finalità probatorie.

Per tutti gli altri scopi, diversi da quelli rientranti nell'art. 349, comma 2, c.p.p., in conformità al regolamento europeo, l'impiego della tecnologia di riconoscimento facciale per perseguire finalità investigative e probatorie, dovrebbe essere subordinato a un provvedimento autorizzativo rilasciato da un'autorità giudiziaria avente funzioni giurisdizionali [24], su richiesta del pubblico ministero, ovvero della polizia giudiziaria, qualora l'attivazione del sistema risulti assolutamente indispensabile ai fini della prosecuzione delle indagini o per la prova di fatti rilevanti.

Per garantire un utilizzo conforme ai principi dello Stato di diritto, la possibilità di attivare il riconoscimento facciale, in entrambe le modalità, dovrebbe essere limitata poi ai casi espressamente previsti dalla legge e circoscritta a specifiche ipotesi di reati gravi, tenendo a mente come punto di partenza le eccezioni elaborate dal regolamento (UE) 2024/1689 all'art. 5, par. 1, lett. h), la cui repressione e accertamento richiedano strumenti investigativi avanzati. La previsione di specifici presupposti normativi, riferibili a fattispecie criminose di elevata offensività e complessità – quali il terrorismo, la criminalità organizzata o i reati connotati da pericolosità sociale diffusa – costituirebbe una modalità di attuazione della riserva di legge in materia di limitazione dei diritti fondamentali, attualmente priva di compiuta implementazione nell'ordinamento italiano. Tale vuoto normativo è reso evidente dalla genericità del quadro attuale, aggravato dal cosiddetto "decreto capienze", che non ha provveduto a colmare tale lacuna, lasciando inattuata la clausola di riserva di legge.

Con specifico riferimento alla modalità di riconoscimento facciale *in tempo reale*, occorrerebbe poi definire i limiti temporali di operatività, escludendo la possibilità di un funzionamento prolungato senza una verifica periodica. Un uso continuativo del sistema, privo di adeguati controlli

[24] Cfr. il capitolo IV, § 3.2.2.

sull'effettiva necessità della misura, risulterebbe incompatibile con i principi di proporzionalità e di stretta necessità. L'estensione del periodo di operatività dello strumento non dovrebbe essere concepita come un automatismo, bensì dovrebbe essere espressamente autorizzata a seguito di una rinnovata valutazione, basata su criteri rigorosi, circa la perdurante sussistenza delle condizioni che avevano inizialmente legittimato l'attivazione del sistema.

L'introduzione di un meccanismo di autorizzazione preventiva assicura un controllo *ex ante* sull'utilizzo della tecnologia, impedendo che il riconoscimento facciale diventi uno strumento di sorveglianza sistematica, privo delle adeguate limitazioni normative. L'ammissione di deroghe al regime autorizzativo prevista dal regolamento in ipotesi di eccezionalità e urgenza non dovrebbe tradursi poi in una possibilità di impiego arbitrario della tecnologia, né in una deresponsabilizzazione dell'autorità giudiziaria nell'esercizio delle sue funzioni di controllo. Per tale motivo, l'uso del riconoscimento facciale senza autorizzazione preventiva dovrebbe essere sottoposto a una verifica successiva da parte di un'autorità indipendente avente il compito di accertare la legittimità dell'urgenza e la corretta applicazione dei criteri di necessità e proporzionalità. In tal senso, il pubblico ministero e le forze di polizia che abbiano attivato il sistema in situazioni di necessità dovrebbero essere obbligati a documentare dettagliatamente le motivazioni che hanno reso impossibile ottenere un'autorizzazione preventiva, offrendo la piena tracciabilità dell'operazione e consentendo una valutazione postuma della sua conformità alle disposizioni normative.

Nell'ottica di garantire un'adeguata tutela dei diritti fondamentali, dovrebbe poi essere prevista la possibilità per l'indagato e/o per il suo difensore di richiedere un contraddittorio tecnico postumo, in modo da rendere possibile una verifica indipendente sulla legittimità dell'acquisizione e sulla certificazione del modello di confronto eventualmente impiegato. In questa prospettiva, la difesa dovrebbe essere messa nelle condizioni di accedere alla documentazione tecnica relativa al sistema di riconoscimento facciale impiegato, con l'indicazione delle metodologie di addestramento; le metriche di accuratezza e il tasso di errore riconosciute a livello tecnico, con riferimento ai margini di falsi positivi e falsi negativi; le condizioni di acquisizione delle immagini di riferimento, inclusi gli aspetti legati alla qualità, all'illuminazione e alla risoluzione del dato biometrico; le modalità di confronto tra il volto acquisito e i dati presenti nel database di riferimento per escludere che vi siano stati errori metodologici o discrepanze nei criteri di *matching*.

Infine, considerata la particolare categoria dei dati trattati da questi strumenti, il legislatore dovrebbe prevedere l'istituzione di un archivio

digitale centralizzato, gestito dalla Procura della Repubblica, con lo scopo di garantire la tracciabilità, la protezione e l'uso esclusivamente dei dati relativi ai *match* positivi stabiliti tra il volto analizzato e i dati biometrici archiviati nel database di riferimento. L'archiviazione dei soli dati oggetto di un *match* positivo garantirebbe un più agevole esercizio dei diritti di accesso, rettifica e cancellazione da parte degli interessati, rendendo possibile un controllo più stringente dalle autorità giudiziarie e dall'Autorità garante per la protezione dei dati personali. In tal modo, si rafforzerebbe anche la legittimità dell'impiego della tecnologia di riconoscimento facciale nel processo penale, ancorando la sua utilizzabilità a una base legale chiara e a meccanismi di controllo giurisdizionale effettivi, come richiesto dalla giurisprudenza costituzionale e sovranazionale in materia di trattamento dei dati personali.

Tali proposte costituiscono soltanto una selezione delle linee direttrici che emergono da riflessioni più ampie riportate nei precedenti capitoli, volte a delineare un quadro normativo capace di coniugare efficacemente l'innovazione tecnologica con la tutela dei diritti fondamentali. È evidente che buona parte degli sforzi regolatori posti in essere a livello sovranazionale, in particolare dall'Unione europea, potrà esplicare una reale efficacia solo nella misura in cui il legislatore nazionale sarà in grado di recepire e tradurre tali impulsi in disposizioni giuridiche chiare, cogenti e conformi ai principi costituzionali interni. L'intervento normativo europeo ha infatti tracciato un percorso preciso, teso a instaurare un sistema armonizzato di regole per l'uso delle tecnologie di riconoscimento facciale, promuovendo standard elevati di protezione dei dati personali, di trasparenza e di responsabilizzazione degli attori istituzionali coinvolti. Tuttavia, è nella fase di attuazione nazionale che si gioca la reale capacità del sistema giuridico di assicurare un bilanciamento adeguato tra le esigenze di sicurezza e quelle di tutela dei diritti inviolabili della persona. L'esito di questo processo normativo – ambizioso e in fase evolutiva – è ancora incerto. Solo il tempo dirà quali saranno gli effetti, ma la strada appare tracciata.

Bibliografia essenziale

ADINI Y.-MOSES Y.-ULLMAN S., *Face recognition: The Problem of Compensating for Changes, in Illumination Direction*, in *IEEE Trans. on Patt. Anal. Mach. Intel.*, 19(7), July 1997, p. 721-732.

ADORNO R., *Il prelievo a fini investigativi*, in *Giur. it.*, III, 2010, p. 1238.

AGOSTINIS S.-CATENACCI B., *Crimini e scrittura. La perizia grafica negli Stati Uniti*, Aras, Pesaro-Urbino, 2012.

AGOSTINO L.-PERALDO M., *Le intercettazioni con captatore informatico: ambito di applicazione e garanzie procedurali*, in *Diritto di Internet, digital copyright and data protection*, suppl. fasc. 3, 2020.

AITKEN C.-TARONI F., *Statistics and the Evaluation of Evidence for Forensic Scientists*, Wiley, New York, 2004.

AITKEN C.-ROBERTS R.-JACKSON G., *Fundamentals of probability and statistical evidence in criminal proceedings: guidance for judges, lawyers, forensic scientists and expert witnesses*, Royal Statistical Society, London, 2010.

ALBANO LEONI F.-MATURI P., *Fonetica sperimentale e fonetica giudiziaria*, in *Giur. it.*, I, 1991.

ALBERINI L., *Sul documento informatico e sulla firma digitale (novità legislative)*, in *Giust. civ.*, 1998.

ALESCI T., *Il corpo umano fonte di prova*, Wolters Kluwer Cedam, Milano, 2017.

ALLEN R. J.-KUHNS B. R.-SWIFT E., *Evidence. Text, problems and cases*, Wolters Kluver, New York, 2012.

ALPA G. (a cura di), *Diritto e intelligenza artificiale. Profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile*, Pacini, Pisa, 2020.

AMATO G., *Individuo e autorità nella disciplina della libertà personale*, Giuffrè, Milano, 1967.

AMATO G., *Commento all'art. 13 Cost.*, in G. BRANCA (a cura di), *Commentario alla Costituzione*, Zanichelli, Bologna, 1977.

AMATO A.-FLORA G.-VALBONESI C., *Scienza, diritto e processo penale nell'era del rischio*, Giappichelli, Torino, 2019.

AMATO S.-CRISTOFARI F.-RACITI S., *Biometria-I codici a barre del corpo*, Giappichelli, Torino, 2013.

AMATO MANGIAMELI A.C., *Algoritmi e big data. Dalla carta sulla robotica*, in *Riv. fil. dir.*, 1, 2019.
AMIDEI A., *Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in *Giur. it.*, 2021.
AMODIO E., *Libertà e legalità della prova nella disciplina della testimonianza*, in *Riv. it. dir. proc. pen.*, 1973.
AMODIO E., *Il dibattimento nel nuovo rito accusatorio*, in *Giust. pen.*, III, 1989, c. 580.
AMODIO E., *Perizia e consulenza tecnica nel quadro probatorio del nuovo processo penale*, in *Cass. pen.*, 1989.
AMODIO E., *Giusto processo, procès équitable e fair trial: la riscoperta del giusnaturalismo processuale in Europa*, in *Riv. it. dir. e proc. pen.*, 1-2, 2003.
AMODIO E., *Processo penale, diritto europeo e common law*, Giuffrè, Milano, 2003.
AMODIO E.-DOMINIONI O., *Commentario del nuovo codice di procedura penale*, vol. I, Giuffrè, Milano, 1989, p. XXXVII.
ANCHETA A.N., *Scientific evidence and equal protection of the law*, Rutgers University Press, New Jersey, 2006.
ANDREOLI A., *Identità alla prova. La controversa storia del test del Dna tra crimini, misteri e battaglie legali*, Sironi, Milano, 2009.
ANDRIOLI V., *Diritto processuale civile*, I, Jovene, Napoli, 1979.
ANGELETTI R., *Il processo indiziario. Indizio, sospetto e congettura al vaglio della giurisprudenza di legittimità*, Giappichelli, Torino, 2021.
APRILE E., *Le indagini tecnico-scientifiche: problematiche giuridiche sulla formazione della prova penale*, in *Cass. pen.*, 2003.
APTEKER R.T.-FISHER J.A.-KISIMOV V.S.-NEISHLOS H., *Video acceptability and frame rate,* in *IEEE MultiMedia,* 2(3), 1995, p. 32-40.
ARONSON D., *Genetic Witness. Science, Law and Controversy in the making of Dna profiling*, Rutgers University Press, New Brunswick, 2007.
ATERNO S., *Acquisizione e analisi della prova informatica*, in *Dir. pen. e proc.*, 2008, *Suppl. Dossier. La prova scientifica nel processo penale.*
ATERNO S., *Le investigazioni informatiche e l'acquisizione della prova digitale*, *Giur. merito*, 4, 2013.
ATERNO S.-CAJANI F.-COSTABILE G.-CURTOTTI D. (a cura di), *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Giappichelli, Torino, 2021.
ATERNO S.-CAJANI F.-COSTABILE G.-MATTIUCCI M.-MAZZARCO G. (a cura di), *Computer forensics e indagini digitali*, Experta, Forlì, 2011.
AURIEMMA M., *Sulla prova "unica o determinante". Il caso Al Khawaja e Tahery c. Regno Unito*, in *Arch. pen.*, 2012, p. 598-600.
AZA A., *Scores as Decisions? Article 22 GDPR and the judgement of the CJEU in SCHUFA Holding (Scoring), in the Labour Context*, in *ILJ*, 2024.

BACCARI G.M.-CONTI C., *La corsa tecnologica tra costituzione, codice di rito e norme sulla privacy: uno sguardo d'insieme*, in *Dir. pen. e proc.*, 6, 2021, p. 711.

BACHMAIER WINTER L., *Mutual Admissibility of Evidence and Electronic Evidence in the EU. A New Try for European Minimum Rules in Criminal Proceedings?* in *Eucrim*, 2, 2023.

BACHMAIER WINTER L.-SALIMI F., *Admissibility of Evidence in EU Cross-Border Criminal Proceedings. Electronic Evidence, Efficiency and Fair Trial Rights*, Hart Publishing, Oxford, 2024.

BACHOO A.K.-TAPAMO J.R., *Texture Detection for Segmentation of Iris Images*, Proceedings of Saicsit, 2005, p. 111-118, su http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.192.6766&rep=rep1&type=pdf.

BALESTRA L., *La dichiarazione giudiziale di paternità e maternità alla luce della riforma della filiazione*, in *Riv. trim. dir. e proc. civ.*, 4, 2014, p. 1223.

BALLERO B., *Tutela sostanziale del diritto di difesa e nuovo corso della giurisprudenza*, in *Giur. cost.*, 1972, p. 997.

BALOSSINO N.-SIRACUSA S., *L'identificazione basata sul volto: metodi fisionomici e metrici*, disponibile su www.itasforum.it/pdf.phf?file=78_7%20-%20Balossino_Siracusa.pdf.

BALSAMO A.-KOSTORIS R.E., *Giurisprudenza europea e processo penale italiano*, Giappichelli, Torino, 2008.

BANDYOPADHYAY D.-SEN J., *Internet of Things: Applications and Challenges in Technology and Standardization*, in *Wirel. Pers. Commun.*, 58(1), 2011, p. 49-69.

BARABASI A.L., *Link. La nuova scienza delle reti*, Einaudi, Milano, 2004.

BARBARO A.-LA MARCA A.-NOBILE E.-ROMEO P., *La prova tecnica nel processo penale. Aspetti pratico scientifici*, Editore Key, Firenze, 2016.

BARBATO V.-LAGO G.-MANZARI V., *Come ovviare al vuoto sui prelievi coattivi creato dalla sentenza n. 238 del 1996*, in *Dir. pen. e proc.*, 3, 1997.

BARBERA A., *Pari dignità sociale e valore della persona umana nello studio del diritto di libertà personale*, in *Iustitia*, 1962.

BARBIERI A., *Le attività d'indagine della polizia giudiziaria su sistemi informatici e telematici*, in *Dir. Internet*, 2008, 5.

BARFIELD W.-PAGALLO U. (eds.), *Research Hanbook on the Law of Artificial Intelligence*, Edward Elgar publishing, Cheltenham-Northampton, 2018.

BARGIS M., *Note in tema di prova scientifica nel processo penale*, in *Riv. dir. proc.*, 2011, p. 47 ss.

BARILE P., *Diritti dell'uomo e libertà fondamentali*, il Mulino, Bologna, 1984.

BARKANE I., *Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance*, in *Information Polity*, 27, 2022.

BARNI M.-TONDI B., *The source identification game: an information-theoretic*

perspective, in *Information Forensics and Security*, *IEEE Transactions* on 8.3, 2013, p. 450-463.
BARONA VILAR S., *Una jusiticia 'digital'y 'algoritmica' para una sociedad en stado de mudanza*, in S. BARONA VILAR (a cura di), *Justicia algoritmica y neuroderecho*, Editorial Tirant Lo Blanch, Valencia, 2021.
BARONE G., *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della Risoluzione del Parlamento europeo del 6 ottobre 2021*, in *Cass. pen.*, 3, 2022, p. 1180.
BARONE G., *La regolamentazione dell'Intelligenza Artificiale: è "corsa agli armamenti"*, in *Dir. pen. e proc.*, 8, 2024.
BARTOLI L., *La catena di custodia del materiale informatico: soluzioni a confronto*, in *Anales de la facultad de derecho*, 33, 2016, p. 145-162.
BARTOLI L., *Parità delle armi e discovery digitale: qualche indicazione da Strasburgo*, in *Leg. pen.*, 13 gennaio 2022.
BASILE F., *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. uomo*, 2019, 10.
BATTIATO S.-GALVAN F., *Ricostruzioni di informazioni 3D a partire da immagini bidimensionali*, in *Sic. e giust.*, IV/MMXIII, 2013, p. 12-14.
BATTIATO S.-BRUNA A.-PUGLISI G., *A Robust Block Based Image/Video Registration Approach for Mobile Imaging Devices*, in *IEEE Transactions on Multimedia*, 12(7), 2010, p. 622-635.
BAUMAN Z., *Dentro la globalizzazione*, Laterza, Roma-Bari, 1998.
BELFATTO E., *La biometria applicata alla sicurezza e al contesto forense*, FDE Institute Press, Mantova, 2015.
BELFIORE R., *Quali prospettive per l'ammissibilità reciproca delle prove fra gli Stati membri dell'Unione europea?*, in *Cass. pen.*, 2023, p. 3870.
BELVINI L., *Videoriprese non investigative e tutela della riservatezza*, in *Proc. pen. giust.*, 4, 2018, p. 797.
BEN ARI D.-FRISH Y.-LAZOVSKI A.-ELDAN U.-GREENBAUM D., *Artificial Intelligence in the Practice of Law: An Analysis and Proof of Concept Experiment*, in 23 *RJL&T*, 2017, p. 21 ss.
BENTHAM J., *Panopticon ovvero la casa d'ispezione*, Marsilio, Venezia, 1983.
BERGGREN S. *et al.*, *Emotion recognition training in autism spectrum disorder: A systematic review of challenges related to generalizability*, in *Dev.Neur.*, 21:3, 2018, p. 141-154.
BERNASCONI A., *La ricognizione di persone nel processo penale. Struttura e procedimento probatorio*, Giappichelli, Torino, 2003.
BERNSTEIN D.E., *Junk Science in the United States and the Commonwealth*, in *Yale J. Int. L.*, 1996.
BERTILLON A., *La Photographie Judiciaire.* Gauthier-Villars et fils, Paris, 1890.
BERTILLON A., *Identification anthropometrique: instruction signaletiques*, Melun, Imprimerie Administrative, 1893.

BESTAGINI P.-ALLAM A.-MILANI S.-TAGLIASACCHI M.-TUBARO S., *Video codec identification*, in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, 2012.

BESTERS M.-BROM F.W.A., *"Greedy" Information Technology: The Digitalization of the European Migration Policy*, in *European Journal of Migration & Law*, 12(4), 2010, p. 462.

BIEGA J.-FINCK M., *Reviving Purpose, Limitation and Data Minimisation in Data-Driven System*, in *Technology and Regulation*, 2021, p. 44-61.

BIGNAMI F. (a cura di), *EU Law in Populist Times*, Cambridge University Press, Cambridge, 2020.

BILIGOTTI N., *Frizioni costituzionali nell'era della sorveglianza: intelligenza artificiale, processo penale e identificazione biometrica*, in *Medialaws*, 16 novembre 2022.

BINNS R.-VEALE M., *Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR*, in *International Data Privacy Law*, II(4), 2021, p. 319-322.

BIRAL M., *L'identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, in *Riv. it. dir. proc. pen.*, 4, 2015, p. 1842.

BISCARETTI DI RUFFIA P., voce *Habeas corpus*, in *Enc. dir.*, XIX, Milano, 1970, p. 941.

BISI S., *Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica*, in *Ciberspazio e diritto*, 6(4), 2005, p. 3-35.

BISSI S., *Biometria e videosorveglianza*, su http://archivio.cnipa.gov.it/site/_files/2007120629641.pdf.

BIZZARRO P.G., *Il futuro è nei dati: data sharing e data spaces nel mercato unico europeo*, disponibile su https://datavalley.it/2021/04/07/il-futuro-e-nei-dati-data-sharing-e-data-spaces-nel-mercato-unicoeuropeo/?fbclid=IwAR3ofkdNg5hQzJeQyMjhYigAqfn0I6vHbH21-pxAFa7i8JgALELpFdRlEbw.

BODEN M.A., *L'intelligenza artificiale*, Il Mulino, Bologna, 2019.

BOLLE R.M.-CONNELL J.H.-PANKANTI S.-RATHA N.K.-SENIOR A.W., *Guide to Biometrics.* Springer-Verlag, New-York, 2003.

BONETTI M., *Riservatezza e processo penale*, Giuffrè, Milano, 2003.

BORGIA G., *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *Leg. pen.*, 11 dicembre 2021.

BÖSE M., *An Assessment of the Commission's Proposal on Electronic Evidence*, reperibile su https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf.

BOVE T.-GIUA P.E.-FORTE A.-ROSSI C., *Un metodo statistico per il riconoscimento del parlatore basato sull'analisi delle formanti*, in *Statistica*, anno LXII, n. 3, 2002.

BOZIO V., *L'ammissibilità nel processo penale di videoriprese effettuate dalla persona offesa*, in *Dir. pen. e proc.*, 2015, p. 585 ss.

BRAMANTI M., *Valutazioni probabilistiche sui riscontri del DNA a scopo di identificazione criminale*, in *La Matematica nella Società e nella Cultura – Rivista dell'Unione Matematica Italiana*, Serie I, II(3), dicembre 2009.

BRANCA G. (a cura di), *Commentario alla Costituzione. Principi fondamentali*, Zanichelli, Bologna, 1975.

BRANDEIS L.D.-WARREN S., *The Right of privacy*, in 4 *Harvard Law Review*, 1890, tradotto da S. Serra, in V. FROSINI (a cura di), *Ius solitudinis*, Giuffrè, Milano, 1993.

BRAVO A., *Argomenti di Grafologia peritale*, ESI, Napoli, 2001.

BRAVO A., *Metodologia della consulenza tecnica e della perizia grafica*, Giordano Editore, Mesagne, 2005.

BRAVO A., *Variazioni naturali e artificiose della grafia*, Giordano Editore, Mesagne, 2005.

BRECKENRIDGE K., *Biometric State. The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*, Cambridge University Press, Cambridge, 2014.

BRIMICOMBE A.J.-MUNGROO P., *Algorithms in the Dock: Should Machine Learning Be Used in British Courts?*, in *Proceedings of the fourth Winchester Conference on Trust, Risk, Information and the Law*, 3 maggio 2017.

BRKAN M., *Do algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond*, in *Electronic Journal*, gennaio 2017.

BROMBA M., *On the Reconstruction of Biometric Raw Data from Template Data*, 2006, https://www.bromba.com/knowhow/temppriv.htm.

BRUSCO C., *Il vizio di motivazione nella valutazione della prova scientifica*, in *Dir. pen. e proc.*, 14, 2004, p. 1414.

BRUSCO C., *La valutazione della prova scientifica*, in *Dir. pen. e proc.*, 2008, *Dossier: La prova scientifica nel processo penale*.

BRUSCO C., *Scienza e processo penale: brevi appunti sulla valutazione della prova scientifica*, in *Riv. it. med. leg. (dal 2012 Riv. it. med. leg. e dir. san.)*, 1, 2012.

BÜCHI M., *Chilling Effects of Profling Activities: Mapping the Issues*, in *CL&SR*, 36, 2020.

BUITEN M.C., DE STREEL A., PEITZ M., *The law and economics of AI liability*, in *Computer Law & Security Review*, 48, 2023, p. 18.

BUOLAMWINI J.-ORDÓÑEZ V.-MORGENSTERN J.-LEARNED-MILLER E., *Facial Recognition Technologies: A Primer*, in *Algorithmic Justice League*, 2020.

BYGRAVE L.A., *Article 22 Automated individual decision-making including profiling*, in C. KUNER *et al.* (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020.

BYGRAVE L.A., *The 'Strasbourg Effect' on data protection in light of the, 'Brussels*

Effect': Logic, mechanics and prospects, in *Computer Law & Security Review*, 40, 2021, 7.

CABIALE A., *I limiti alla prova nella procedura penale europea*, Wolters Kluwer Cedam, Milano, 2019.

CABIALE A., *L'Acquisizione delle intercettazioni con procedura di controllo giudiziale: ritorni al passato e nuove lacune*, in *Diritto di Internet*, *digital copyright and data protection*, suppl. fasc. 3, 2020.

CADOPPI A.-CANESTRARI S.-MANNA A.-PAPA M. (a cura di), *Cybercrime, Trattati giuridici Omnia,* Utet giuridica, Milano, 2019.

CAGGIANO G., *L'interoperabilità fra le banche dati dell'Unione sui cittadini degli Stati terzi*, in *Dir., imm., citt.*, 1, 2020, p. 180.

CAIANIELLO M., *Dal terzo pilastro ai nuovi strumenti: diritti fondamentali, "road map" e l'impatto delle nuove direttive*, in *I nuovi orizzonti della giustizia penale europea*, *Atti del convegno. Milano, 24-26 ottobre 2014*, Giuffrè, Milano, 2015.

CAIANIELLO M., *L'OEI dalla direttiva al decreto n. 108 del 2017*, in M. DANIELE-R.E. KOSTORIS (a cura di), *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017*, Giappichelli, Torino, 2018.

CAIANIELLO M., *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *EJCCL& CJ*, 29, 2021, 1-23.

CAIANIELLO M.-CAMON A. (a cura di), *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations*, Wolters Kluwer Cedam, Milano, 2021.

CAIN S.-SMRKOVSKY L.-WILSON M., *Voiceprint Identification*, si veda http://expertpages.com/news/voiceprint_identification.html.

CAJANI F., *Il vaglio dibattimentale della digital evidence*, in *Arch. pen.*, 3, 2013, p. 837-852.

CALAMANDREI I., *La prova documentale*, Cedam, Padova, 1995.

CALAMANDREI P., *Il giudice e lo storico*, in *Riv. dir. proc.*, 1939.

CALLARI F.-COPPOLA V., *Il contraddittorio nella formazione della prova scientifica in dibattimento e il deposito preventivo delle perizie e delle consulenze tecniche*, in *Cass. pen.*, 10, 2023, p. 3047.

CALOGERO G., *La logica del giudice e il suo controllo in Cassazione*, Cedam, Padova, 1937.

CAMALDO L., *La direttiva sull'ordine europeo di indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione*, in *Dir. pen. cont.*, 27 maggio 2014.

CAMON A., *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen.*, 4, 1999, p. 1188.

CAMON A., *Le Sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi*, in *Riv. it. dir. e proc. pen.*, 2006, p. 1550.
CANZIO C., *Prova scientifica, ricerca della "verità" e decisione giudiziaria nel processo penale*, in C. DE MAGLIE-S. SEMINARA (a cura di), *Scienza e casualità*, Cedam, Padova, 2006.
CAMON A., *La disciplina delle indagini genetiche*, in *Cass. pen.*, 4, 2014, p. 1426.
CAMON A., *La prova genetica tra prassi investigative e regole processuali*, in *Proc. pen. giust.*, 6, 2015, p. 165 ss.
CANZIO G., *Prova scientifica, ragionamento probatorio e libero convincimento del giudice nel processo penale*, in *Dir. pen. e proc.*, 2003, p. 1200.
CANZIO G., *L'"oltre il ragionevole dubbio" come regola probatoria e di giudizio nel processo penale*, in *Riv. it. dir. proc. pen.*, 2004, p. 305.
CANZIO G., *La causalità fra diritto e processo penale*, in *Cass. pen.*, 2007, p. 1324.
CANZIO G., *Intelligenza artificiale e processo penale*, in *Cass. pen.*, 3, 2021, p. 797.
CANZIO G., *Intelligenza artificiale, algoritmi e giustizia penale*, in *Sist. pen.*, 8 gennaio 2021.
CANZIO G., *AI Act e processo penale: sfide e opportunità*, in *Sist. pen.*, 14 ottobre 2024.
CANZIO G.-LUPARIA L. (a cura di), *Prova scientifica e processo penale*, Wolters Kluwer Cedam, Milano, 2018.
CANZIO G.-LUPARIA L. (a cura di), *Prova scientifica e processo penale*, Wolters Kluwer Cedam, Milano, 2022.
CAO Q.-SHEN L.-XIE W.-PARKHI O.M.-ZISSERMAN A., *VGGFace2: a dataset for recognising faces across pose and age*, in *International Conference on Automatic Face and Gesture Recognition*, 2018.
CAPRIOLI F., *Colloqui riservati e prova penale*, Giappichelli, Torino, 2000.
CAPRIOLI F., *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2009.
CAPRIOLI F., *Scientific evidence e logiche del probabile nel processo per il "delitto di Cogne"*, in *Cass. pen.*, 2009.
CAPRIOLI F., *Verità e giustificazione nel processo penale*, in *Rev. Bras. de Dir. Proc. Pen.*, 3(1), 2017.
CARDARELLI F.-SICA S.-ZENCOVICH V.Z., *Il codice dei dati personali. Temi e problemi*, Giuffrè, Milano, 2004.
CARETTI P.-DE SIERVO V., *Istituzioni di diritto pubblico*, Giappichelli, Torino, 2006.
CARLEO A. (a cura di), *Decisione robotica*, il Mulino, Bologna, 2019.
CARLI GARDINO A., *Il diritto di difesa nell'istruttoria penale: saggio sull'art. 24 comma 2 Cost.*, Giuffrè, Milano, 1983.
CARLIZZI G., *Giudice 2.0 e uso del sapere specialistico nel processo penale*, in *Proc. pen. e giust.*, 4, 2017, p. 732-754.

CARLIZZI G., *La valutazione della prova scientifica*, Giuffrè, Milano, 2019.
CARLIZZI G.-TUZET G., *La prova scientifica nel processo penale*, Giappichelli, Torino, 2018.
CARNELUTTI F., *La prova civile*, Athenaeum, Roma, 1915.
CARNELUTTI F., *Lezioni sul processo penale*, vol. I, Società Editrice Temi, Roma, 1946.
CARNELUTTI F., *Principi del processo penale*, Giuffrè, Milano, 1960.
CARNELUTTI F., *Prova del sangue*, in *Riv. dir. proc.*, 1961, p. 129 ss.
CAROFIGLIO G., *L'arte del dubbio*, Sellerio, Palermo, 2007.
CARPONI SCHITTAR D.H.L., *Modi dell'esame e del controesame*, vol. I, Giuffrè, Milano, 1992.
CARRATTA A.-DE CARO M.-PINO G. (a cura di), *Intorno al ragionamento giuridico*, Romatre-Press, Roma, 2022.
CARRER L., *La Russia usa il riconoscimento facciale su chi manifesta contro la guerra*, 16 marzo 2022, in www.wired.it.
CARRER L., *Black Box. Sicurezza e sorveglianza nelle nostre città*, Ledizioni, Milano, 2023.
CARRETTA P.-CILLI A.-IACOVIELLO A.-GRILLO A.-TROCCHI F., *L'acquisizione del documento informatico. Indagini penali e amministrative*, Laurus Robuffo, Roma, 2012.
CARRIER B.D., *Defining digital forensic examination and analysis tool using abstraction layers*, in *International Journal of Digital Evidence*, 1, 4, 2003, p. 1-12.
CARVALHO D.V.-PEREIRA E.M.-CARDOSO J.S., *Machine Learning Interpretability: A Survey on Methods and Metrics*, in *Electronics*, 8, 2019, p. 832.
CASASOLE F., *Le indagini tecnico-scientifiche: un connubio tra scienza e diritto in perdurante attesa di disciplina*, in *Dir. pen. e proc.*, 11, 2008, p. 1443.
CASCETTA F.-DE LUCCIA M., *Sistemi d'identificazione personale*, in *Il mondo Digitale*, 2004, reperibile su http://archivio-mondodigitale.aicanet.net/Rivista/04_numero_due/Cascetta_p.44-55.pdf.
CASCIONE C.M., *La data retention tra lotta al crimine e aspettative di privacy*, in *Giustiziacivile.com*, 4, 2, 23 febbraio 2017.
CASEY E., *Digital Evidence and Computer Crime. Forensic science, computer and the Internet*, II ed., Elsevier Academic Press, Amsterdam, 2004.
CASIRAGHI R., *Testimoni assenti: la Grande camera ridefinisce la regola della 'prova unica o determinante'*, in *Cass. pen.*, 2012, p. 3116.
CASONATO C., *Intelligenza artificiale e giustizia: potenzialità e rischi*, in *DPCE online*, 44(3), 2020.
CASSANO G.-CIMINO I.P., *Diritto dell'internet e delle nuove tecnologie telematiche*, Cedam, Padova, 2009.
CASTELLI C.-PIANA D., *Giustizia predittiva. La qualità della giustizia in due tempi*, in *Quest. giust.* (web), 3 luglio 2019.
CATALANO E., *L'accertamento dei fatti processuali*, in *Ind. pen.*, 2002.

CATANESI R.-MARTINO V., *Verso una psichiatria forense basata su evidenza*, in *Riv. it. med. leg.*, 2006, p. 1011.

CATH C.-WACHTER S.-MITTELSTADT B.-TADDEO M.-FLORIDI L., *Artificial Intelligence and the 'Good Society': the US, EU, and UK approach*, in *Science and Eng. Ethics*, 2018.

CAULI N.-ORTIS A.-BATTIATO S., *Fooling a Face Recognition System with a Marker-Free Label-Consistent Backdoor Attack*, in *Image Analysis and Processing-ICIAP 2022: 21st International Conference*, Lecce, Italy, May 23-27, 2022, Proceedings, Part II, p. 176-185.

CECCHI M., *La "motivazione rafforzata" del provvedimento ovvero la "forza persuasiva superiore"*, in *Dir. pen. e proc.*, 2019, p. 1123 ss.

CECCHI M., *La motivazione rafforzata del provvedimento: un nuovo modello logico-argomentativo di stilus curiae*, Wolters Kluwer Cedam, Milano, 2021.

CELORIA E.-FERRARIS V., *Eurodac: dalla gestione delle domande di protezione internazionale al controllo della mobilità*, in *Quad. AISDUE-Riv. quadr.*, fasc. spec. 4, 2024, *Il futuro del diritto e della politica migratoria europea: il Nuovo Patto e oltre*, p. 1-24.

CENTONZE F., *Scienza "spazzatura" e scienza "corrotta" nelle attestazioni e valutazioni dei consulenti tecnici nel processo penale*, in *Riv. it. dir. proc. pen.*, 2001, p. 1232 ss.

CESARI C., *L'impatto delle nuove tecnologie sulla giustizia penale: un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, Porto Alegre, 5(3), 2019, p. 1167-1188.

CESARI C., *L'irripetibilità sopravvenuta degli atti di indagine*, Giuffrè, Milano, 1999.

CHAN G.K.Y., *Towards a calibrated trust-based approach to the use of facial recognition technology*, in *International Journal of Law and Information Technology*, 2021, p. 1-27.

CHANG Y.-ZHANG W.-CHEN T., *Biometric-based cryptographic key generation*, in *Proceedings of IEEE International Conference on Multimedia and Expo (ICMÈ04)*, Taipei, vol. 3, 2004, p. 2203-2206.

CHAPMAN R.B., *Admissibility of Voiceprints Not Limited to "Corroborative Purposes", United States v. Franks*, 511 F.2d 25 (6th Cir. 1975), in *Akron Law review*, si veda https://www.uakron.edu/dotAsset/d1e99bd8-b0df-40b3-9637-1a9084acb737.pdf.

CHELO A., *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia giudiziaria*, Wolters Kluwer Cedam, Milano, 2014.

CHELO A., *La tutela della libertà morale nella formazione della prova penale*, Cedam, Wolters Kluwer Cedam, Milano, 2025.

CHESSMAN C., *A source of error: computer code, criminal defendants, and the constitution*, in *Calif. Law Rev.*, 2016, p. 179-228.

CHIAVARIO M., *Processo e garanzie della persona*, vol. II, Giuffrè, Milano, 1984.

CHIAVARIO M., *La riforma del processo penale*, II ed., Giappichelli, Torino, 1990.
CHIAVARIO M. (a cura di), *Commento al nuovo codice di procedura penale*, Utet, Torino, 1991.
CHIAVARIO M., voce *Libertà personale (dir. proc. pen.)*, in *Enc. giur.*, Roma, 1993.
CHIAVARIO M., *Considerazioni sul diritto alla prova*, in *Cass. pen.*, 1996, p. 2009.
CHIAVARIO M., *sub art. 6 Cedu*, in S. BARTOLE-B. CONFORTI-G. RAIMONDI, *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, Cedam, Padova, 2001.
CHIAVARIO M., voce *"Giusto processo" (proc. pen.)*, in *Enc. giur.*, Roma, 2001, 1.
CHIAVARIO M., *Diritto processuale penale. Profilo istituzionale*, II ed., Utet, Torino, 2006.
CHIAVARIO M., *Diritto processuale penale*, IX ed., Utet giuridica, Milano, 2022.
CHIAVARIO M., *Diritto processuale penale*, X ed., Giappichelli, Torino, 2024.
CHIAVARIO M.-MARZADURI E. (a cura di), *Giurisprudenza sistematica di diritto processuale penale*, Giappichelli, Torino, 1999.
CISTERNA A., *Perquisizioni in caso di fondato motivo*, in *Guida dir.*, 2008.
CLARKE R., *Biometric's Inadequacies and Threats, and the Need for the Regulation*, 15 aprile 2002, disponibile su http://www.rogerclarcke.com/DV/BiomThreats.html.
COATS W. S.-BAGDASARIAN A.-HELOU T.J.-LAM T., *The Practitioner's Guide to Biometrics*, American Bar Association, Chicago, 2007.
COLACURCI M., *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sist. pen.,* 9, 2022.
COLAIACOVO G. (a cura di), *Sicurezza, informazioni e giustizia penale,* Pacini giuridica, Pisa, 2023.
COLAIOCCO A., *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria*, in *Arch. pen.*, 1, gennaio-aprile 2019 (online).
COLAROCCO V.-GROTTO T.-VACIAGO G., *La prova digitale. La casistica civile e penale gli strumenti di acquisizione in ambito* cloud, Giuffrè, Milano, 2020.
COLE S.A., *Is Fingerprint Identification Valid? Rhetorics of Reliability in Fingerprint Proponents' Discourse*, in *Law & Policy*, 28(1), January 2006, p. 116.
COLOGGI F., *Identità personale: filosofia, scienza e criminologia*, in *Profiling. I profili dell'abuso. Giornale scientifico a cura dell'O.N.A.P.*, anno 1, n. 4, dicembre 2010, su http://www.onap-profiling.org/?p=853.
COLOMBO E., *Una novità dall'Unione Europea per la lotta ai Cybercrimes: una Electronic Evidence Guide*, in *Cass. pen.*, 2014, p. 374 ss.

COMOGLIO L.P., *Prove ed accertamento dei fatti nel nuovo c.p.p.*, in *Riv. it. dir. proc. pen.*, 1990, p. 119.
CONFORTI A., *Controesame di testi della controparte su circostanze non indicate e nuove interpretazioni del diritto alla prova contraria*, in *Cass. pen.*, 1998, p. 2038.
CONSO G., *I fatti giuridici processuali penali*, Giuffrè, Milano, 1955.
CONSO G., *Considerazioni in tema di contraddittorio nel processo penale italiano*, in *Riv. it. dir. proc. pen.*, 1966, p. 405.
CONSO G. (a cura di), *Studi di diritto processuale penale*, Giuffrè, Milano, 1980.
CONSO G.-GREVI V.-BARGIS M. (a cura di), *Compendio di Procedura Penale*, Wolters Kluwer Cedam, Padova, 2014.
CONSO G.-GREVI V.-NEPPI MODONA G., *Il nuovo codice di procedura penale. Dalle leggi delega ai decreti delegati*, vol. I, Cedam, Padova, 1989.
CONSO G.-GREVI V.-NEPPI MODONA G., *Il nuovo codice di procedura penale. Dalle leggi delega ai decreti delegati*, vol. IV, Cedam, Padova, 1989.
CONSOLO O., voce *Perito ed interprete (dir. proc. pen.)*, in *Enc giur.*, XIII, Roma, 1990, p. 2.
CONTALDO A., *Biometrie e documenti di viaggio: problematiche giuridiche in campo*, in *Riv. amm. Rep. it.*, 6, 2006, p. 545 ss.
CONTI C., *Le due anime del contraddittorio nel nuovo art. 111 Cost.*, in *Dir. pen. e proc.*, 2000.
CONTI C., *Le videoriprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi "riservati"*, in *Dir. pen. e proc.*, 2006, p. 1347 ss.
CONTI C., *Il processo si apre alla scienza. Considerazioni sul procedimento probatorio e sul giudizio di revisione*, in *Riv. it. dir. proc. pen.*, 2010, p. 1204 ss.
CONTI C., *Il volto attuale dell'inutilizzabilità: derive sostanzialistiche e bussola della legalità*, in *Dir. pen. e proc.*, 2010, p. 790 ss.
CONTI C., *La riservatezza delle intercettazioni nella "delega Orlando"*, in *Dir. pen. cont.*, 3, 2017, p. 78 ss.
CONTI C. (a cura di), *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, Giuffrè, Milano, 2011.
CONTI C., *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen. e proc.*, 9, 2018, p. 1210 ss.
CONTI C., *Scienza controversa e processo penale: la Cassazione e il "discorso sul metodo"*, in *Dir. pen. e proc.*, 6, 2019, p. 848.
CONTI C., *Il "diritto delle prove scientifiche": percorsi metodologici della giurisprudenza nell'era post Franzese*, in *Cass. pen.*, 4, 2022, p. 1644.
CONTI C., *Il principio di non sostituibilità: il sistema probatorio tra costituzione e legge ordinaria*, in *Cass. pen.*, 2, 2024, p. 451.
CONTI C.-TONINI P., *Il diritto delle prove penali*, Giuffrè, Milano, 2014.

CONTI S., *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Inf. e dir.*, anno XLI, XXIV (1-2), 2015, p. 153-164.
CONTI S.-PERUGINELLI G., *L'impatto del regolamento europeo in materia di protezione dei dati personali sull'attività giurisdizionale*, in *Ciber. e dir.*, 1-2, 2018, p. 123 ss.
CONTISSA S.-LASAGNI G.-SARTOR G., *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Dir. Internet*, 4, 2019, p. 619 ss.
CORASANITI M., *La banca dati del DNA: primi aspetti problematici dell'attuazione del Trattato di Prüm*, in *Dir. inf.*, 3, 2009, p. 437.
CORBETTA S., *Commento all'art. 508 c.p.p.*, in A. GIARDA-G. SPANGHER (a cura di), *Codice di procedura penale commentato*, Ipsoa, Milano, 2007, p. 4478 ss.
CORDERO F., *Tre studi sulle prove penali*, Giuffrè, Milano, 1963.
CORDERO F., *Ideologie del processo penale*, Giuffrè, Milano, 1966.
CORDERO F., *Codice di Procedura penale commentato*, Giappichelli, Torino, 1990.
CORDERO F., *Procedura penale*, Giuffrè, Milano, 2003.
COSTABILE G., *Scena criminis, documento informatico e formazione della prova penale*, in *Dir. inf. e inform.*, 2005.
CREEMERS R., *China's Social Credit System: An Evolving Practice of Control*, in *SSRN*, 9 maggio 2018, p. 1-32.
CREMONESI L., *Indagini e garanzie nel sistema americano*, Laurus Robuffo, Roma, 2010.
CRICRÌ L., voce *Videoregistrazioni*, in *Enc. giur.*, XXXII, Roma, 2006.
CUCCI M.-GENNARI G.-GENTILOMO A. (a cura di), *L'uso della prova scientifica nel processo penale*, Maggioli, Santarcangelo di Romagna, 2012.
CUOMO L., *Profili giuridici del trattamento biometrico dei dati*, in *Riv. it. med. leg. (e dir. san)*, 1, 2014, p. 43.
CUOMO L.-RAZZANTE R., *La nuova disciplina dei reati informatici*, Giappichelli, Torino, 2009.
CURRAO E., *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Dir. pen. uomo*, 19 maggio 2021.
CURTI S.-FALCINELLI D., *Tra diritto e scienza: i saperi e la prova nel processo penale*, Wolters Kluwer Cedam, Padova, 2014.
CURTOTTI D.-SARAVO L. (a cura di), *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, e scienze*, Giappichelli, Torino, 2019.
CURTOTTI NAPPI D.-SARAVO L., *L'errore tecnico-scientifico sulla scena del crimine. L'errore inevitabile e le colpe dello scienziato, del giurista, del legislatore*, in *Arch. pen.*, 3, 2011.
CZERNIAWSKI J.-BOYACK C., *Reviewing the Privacy Implications of Law Enforcement Access to and Use of Digital Data*, in *5 Utah J. Crim. L.*, 73, 2021.

D'ALBERGO E.-FASCIANI T.-GIOVANELLI G., *La governance dell'Intelligenza Artificiale nelle politiche locali: trade-off e potere nel caso della videosorveglianza a Torino*, in *Riv. trim. di sc. amm.*, 4, 2023.
D'ALESSIO R., *Sub art. 348*, in G. LATTANZI-E. LUPO (a cura di), *Codice di procedura penale. Rassegna di giurisprudenza e dottrina*, vol. V, Giuffrè, Milano, 2017.
DALFINO D., *Stupidità (non solo) artificiale, predittività e processo*, in *Quest. giust.* (web), 3 luglio 2019.
D'ALFONSO G., *Intelligenza artificiale e responsabilità civile. Prospettive europee*, in *Rev. de Est. Jur. y Crim.*, 2022, p. 163-195.
DALIA A.A. (a cura di), *Le nuove norme di contrasto al terrorismo*, Giuffrè, Milano, 2006.
DAMASKA M., *Il diritto delle prove alla deriva*, il Mulino, Bologna, 2003.
DANIELE M., *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2, 2011, p. 284 ss.
DANIELE M., *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012.
DANIELE M., *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *Cass. pen.*, 2013, p. 367 ss.
DANIELE M., *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale*, in *Dir. pen. cont.-Riv. trim.*, 4, 2015, p. 86 ss.
DANIELE M., *Habeas Corpus. Manipolazioni di una garanzia*, Giappichelli, Torino, 2017.
DANIELE M., *L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul d. lgs. n. 108 del 2017*, in *Dir. pen. cont.*, 7-8, 2017, p. 208 ss.
DANIELE M., *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Rev. Bras. de Direito Processual Penal*, Porto Alegre, 5(3), 2019, p. 1277-1296.
D'AMBROSIO L.-VIGNA P.L., *La pratica di polizia giudiziaria*, Cedam, Padova, 1998.
D'ARIENZO A., *Raccolta di appunti di criminalistica*, in *Sez. Identità Personale – Dattiloscopia*, disponibile su www.officeitalia.it/scicosi/datt.html.
D'AURIA L., *Accertamento oltre il ragionevole dubbio, rispetto del contraddittorio e criteri di verifica dell'attendibilità delle ipotesi scientifico tecniche come principi fondanti il "giusto processo". Risvolti sulla prova penale scientifica e gli accertamenti tecnici*, in *Foro ambr.*, 2003.
D'AURIA L., *Blood pattern Analisys e ragionamento del giudice*, in *Giust. pen.*, 2006, c. 220.
D'AURIA L., *Prova penale scientifica e "giusto processo"*, in *Giust. pen.*, 2004, c. 20.
DE BRUYNE J.-DHEU O.-DUCUING C., *The European Commission's approach to extra-contractual liability and AI – An evaluation of the AI liability directive and the revised product liability directive*, in *CL&SR*, 51, 2022.

DE CATALDO NEUBERGER L., *Psicologia della testimonianza e prova testimoniale*, Giuffrè, Milano, 1988.
DE CATALDO NEUBURGER L. (a cura di), *La prova scientifica nel processo penale*, Cedam, Padova, 2007.
DE CATALDO NEUBERGER L., *Esame e controesame nel processo penale. Diritto e psicologia*, II ed., Cedam, Padova, 2008.
DE CESARIS A.M., voce *Habeas corpus*, in *Enc. giur.*, XIX, Roma, 1991.
DE FLAMMINEIS S., *Le sfide della prova digitale: sequestro, chat, processo penale telematico e intelligenza artificiale*, in *Sist. pen.*, 8 marzo 2024.
DEGANELLO M., *I criteri di valutazione della prova penale. Scenari di diritto giurisprudenziale*, Giappichelli, Torino, 2005.
DE GREGORIO G., *The Digital Services Act: A Paradigmatic Example of European Digital Constitutionalism*, in *Dir. comp.*, 17 maggio 2021, p. 1-6.
DE GREGORIO G.-DUNN P., *The European risk-based approaches: Connecting constitutional dots in the digital age*, in *Common Market Law Review*, 59(2), 2022, p. 473-500.
DE HERT P., *Biometrics: legal issues and implications, in Background paper for the Institute of Prospective Technological Studies*, in *DG JRC-Sevilla, European Commission*, 2005.
DE HERT P.-BOUCHAGIAR G., *European Biometric Surveillance, Concrete Rules, and Uniform Enforcement Beyond Regulatory Abstraction and Local Enforcement*, in R. MATULIONYTE-M. ZALNIERIUTE (eds.), *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge University Press, Cambridge, 2024.
DELAC K.-GRGIC M., *A survey of biometric recognition methods*, in *46th International Symposium Electronics in Marine*, *ELMAR-2004*, 2004, Zadar, Croatia.
DEL BIMBO A. (a cura di), *Pattern Recognition. ICPR International Workshops and Challenges*, ICPR 2021, vol. 12663, Springer, Cham.
DE LEO F., *Le indagini tecniche di polizia: un invito al legislatore*, in *Cass. pen.*, 1996, p. 697 ss.
DEL COCO M.-CARCAGNÌ P., *Face recognition algorithms: performance evaluation*, su https://www.parsec326.it/images/doc/Report_Reco-Performance-Evaluation---CNR.PDF.
DEL GATTO S., *La governance delle nuove tecnologie tra tentativi di regolazione e istanze di self regulation. Il caso del riconoscimento facciale*, in *Riv. it. dir. pubbl. com.*, 2023, p. 42 ss.
DELLA TORRE J., *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del garante privacy d'oltremanica)*, in *Sist. pen.*, 28 marzo 2020.
DELLA TORRE J., *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. e proc. pen.*, 2022, p. 1057-1093.
DELLA TORRE J., *Algoritmi di facial recognition e procedimento penale italiano*,

in I. MICHELI (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*, EUT Edizioni Università di Trieste, Trieste, 2023, p. 167-181.

DE MINICO G., *Giustizia e intelligenza artificiale: un equilibrio mutevole*, in *Riv. AIC*, 2, 2024.

DENNIS I.H., *AlKhawaja and Tahery v United Kingdom, Commentary*, in *Crim. Law Rev.*, 2012, p. 376-378.

DENTI V., *Scientificità della prova e libera valutazione del giudice*, in *Riv. dir. proc.*, 1972.

DEVARAM R.R.-ORTIS A.-BATTIATO S.-BRUNA A.R.-TOMASELLI V., *Real-Time Thermal Face Identication System for Low Memory Vision Applications Using CNN*, in *Pattern Recognition. ICPR International Workshops and Challenges*, Springer Professional, Città, 2021.

DEWEY M., *Classificazione decimale Dewey*, trad. a cura di L. Crocetti, D. Danesi, vol. II, AIB, Roma, 1993.

DI BITONTO M.L., *Le riprese video domiciliari al vaglio delle Sezioni unite*, in *Cass. pen.*, 2006, p. 4344.

DI CHIARA G., *Le linee prospettiche del difendersi ricercando: luci e ombre delle "nuove" investigazioni difensive*, in *Leg. pen.*, 2002, p. 20 ss.

DI NICOLA V., *La libertà personale dell'imputato tra regole smesse, disciplina attuale e sistema futuro*, Boccia, Salerno, 1989.

DI PAOLO G., *La circolazione dei dati personali nello spazio giudiziario europeo dopo Prüm*, in *Cass. pen.*, 2010, p. 1969 ss.

DI PAOLO G., *Tecnologie del controllo e prova penale. L'esperienza statunitense e spunti per la comparazione*, Cedam, Padova, 2008.

DI PAOLO G., voce *Prova informatica (diritto processuale penale)*, in *Enc. dir.*, *Annali*, VI, Milano, 2013.

DI PIETRO A.-CAIANIELLO M. (a cura di), *Indagini penali e amministrative in materia di frodi IVA e doganali. L'impatto dell'European Investigation Order sulla cooperazione transnazionale*, Cacucci, Bari, 2016.

DIXON P., *A Failure to "Do No Harm". India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in *Health Technol.* 7, 2017, p. 539-567.

DOBOSZ M.-CARNEVALI E.-LANCIA M. (a cura di), *Genetica forense e diritto: prospettive scientifiche, tecnologiche e normative*, Giuffrè, Milano, 2011.

DODGE D., *Novel Warrant IDS Suspect Only by DNA Databank Evidence Used to Charge «John Doe» Rape*, in *Milwakee J.E. Sentinel*, 1999.

DOMENICI R., voce *Prova del DNA*, in *Dig. disc. pen.*, X, Torino, 1995.

DOMINIONI O., *sub art. 27 comma 2 Cost.*, in G. BRANCA (a cura di), *Commentario della Costituzione*, Zanichellli-Foro italiano, Bologna-Roma, 1991, p. 212 ss.

DOMINIONI O., *In tema di nuova prova scientifica*, in *Dir. pen. e proc.*, 2001.
DOMINIONI O., *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2005.
DOMINIONI O., *L'esperienza italiana di impiego della prova scientifica nel processo penale*, in *Dir. pen. e proc.*, 5, 2015, p. 601.
DONATI F., *Intelligenza artificiale e giustizia*, in *Riv. AIC*, 1, 2 marzo 2020, p. 415 ss.
DONDI A., *Paradigmi processuali ed "expert witness testimony" nel diritto statunitense*, in *Riv. trim. dir. proc. civ.*, 1996, p. 261 ss.
DONDI E., *Problemi di utilizzazione delle "conoscenze esperte" come expert witness testimony nell'ordinamento statunitense*, in *Riv. trim. dir. proc. civ.*, 2001, p. 1191 ss.
DUGELAY J.L.-JUNQUA J.C.-KOTROPOULOS C.-KUHN R.-PERRONNIN F.-PITA I., *Recent advances in biometric person authentication*, vedi http://www.eurecom.fr/fr/publication/830/download/mm-dugeje-020513.pdf.
DURANTE M.-PAGALLO U., *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet, Torino, 2012.
DUTTA A., *Predicting Performance of a Face Recognition System Based on Image Quality*, PhD thesis, University of Twente, Netherlands, 2015.

EBERS M., *Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act*, in L.A. DIMATTEO-M. CANNARSA-C. PONCIBÒ (eds.), *The Cambridge Hankdbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, Cambridge University Press, Cambridge, 2022.
EBERS M.-CANTERO GAMITO M. (eds.), *Algorithmic Governance and Governance of Algorithms, Legal and Ethical Challenges*, Springer, Berlin, 2020.
EBERS M.-NAVAS NAVARRO S. (eds.), *Algorithms and Law*, Cambridge University Press, Cambridge, 2020.
EBERS M.-HOCH V.R.S.-ROSENKRANZ F.-RUSCHEMEIER H.-STEINRÖTTER B., *The European Commission's Proposal for an Artificial Intelligence Act–A Critical Assessment by Members of the Robotics and AI Law Society*, in *(RAILS). J.*, 4(4), 2021, p. 589-603.
EKMAN P., *Universality of Emotional Expression? A Personal History of the Dispute*, in P. EKMAN (ed.), *The Expression of the Emotions in Man and Animals*, III ed., Oxford University Press, New York, 1998.
EL KHOBBY R.-ABD-ELNABY H.A. *et al.*, *Gait identification by convolutional neural networks and optical flow*, in *Multimed Tools Appl*, 78, 2019, p. 25873-25888.

FAGGIOLI G.-GHIRARDINI A., *Computer Forensics*, Apogeo, Milano, 2009.

FAIGMAN D., *Legal alchemy. The use and the misuse of the science in the law*, W.H. Freeman, New York, 2001.
FAIGMAN D.L.-PORTER E.-SACKS M.J., *Cheek your Cristal Ball at the Courthouse Door, Please: Exploring the Past, Understanding the Present, and Worrying about the Future of Scientific Evidence*, in 15 *Cardozo L. Rev.*, 1803 (1994).
FALATO F., *L'inferenza generata dai sistemi esperti e dalle reti neurali nella logica giudiziale*, in *Arch. pen.*, 2, 2020.
FALETTI E., *Face detection: per la prima volta il riconoscimento al vaglio dei tribunali*, in *Quot. giur.*, 29 ottobre 2019.
FANCHIOTTI V., *Lineamenti del processo penale statunitense*, Giappichelli, Torino, 1987.
FANUELE C., *L'indagine genetica nell'esperienza italiana ed in quella inglese*, in *Riv. it. dir. proc. pen.*, 2006, p. 732 ss.
FANUELE C., *Dati Genetici e procedimento penale*, Cedam, Padova, 2009.
FANUELE C., *La localizzazione satellitare nelle investigazioni penali*, Wolters Kluwer Cedam, Milano, 2019.
FARANDA A., *L'implementazione di sistemi di AI per la sorveglianza nei luoghi pubblici: il caso del Comune di Trento*, in *MediaLaws*, 16 aprile 2024.
FASANO G., *L'interpretazione estensiva della nozione di "decisione automatizzata" ad opera della Corte di giustizia: una prospettiva più ampia ma ancora fragili tutele per le libertà fondamentali*, in *Riv. it. inf. e dir.*, 6, 2, 2024, p. 563 ss.
FASOLIN S., *La copia di dati informatici nel quadro delle categorie processuali*, in *Dir. pen. e proc.*, 2012.
FATTORINI P.-CORRADI F.-RICCI U.-PREVIDERÈ C., *La prova del Dna per la ricerca della verità. Aspetti giuridici, biologici e probabilistici*, Giuffrè, Milano, 2006.
FELICIONI P., *Le ispezioni e le perquisizioni*, Giuffrè, Milano, 2004.
FELICIONI P., *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Ipsoa, Milano, 2007.
FELICIONI P., *L'Italia aderisce al Trattato di Prüm: disciplinata l'acquisizione e l'utilizzazione probatoria dei profili genetici*, in *Dir. pen. e proc.*, *Dossier: Banca dati nazionale del DNA e prelievo di materiale biologico*, 2009.
FELICIONI P., *Art. 188*, in A. GIARDA-G. SPANGHER (a cura di), *Codice di procedura penale commentato*, I, Wolters Kluwer, Milano, 2017.
FELICIONI P., *La prova del Dna nel procedimento penale. Profili sistematici, dinamiche probatorie, suggestioni mediatiche*, Giuffrè, Milano, 2018.
FERRAJOLI L., *Diritto e Ragione – Teoria del garantismo penale*, Laterza, Bari, 1998.
FERRARESI M., *L'effetto CSI può fregare DSK*, in *Il Foglio*, 24 maggio 2011.
FERRUA P., voce *Difesa (diritto di)*, in *Dig. disc. pen.*, III, Torino, 1989, p. 466.

FERRUA P., *Studi sul processo penale*, vol. II, *Anamorfosi del processo accusatorio*, Giappichelli, Torino, 1992.
FERRUA P., *Il "giusto processo"*, Zanichelli, Bologna, 2010.
FERRUA P., *La prova nel processo penale*, I, *Struttura e procedimento*, Giappichelli, Torino, 2017.
FERRUA P.-GRIFANTINI F.M., *La prova nel dibattimento penale*, Giappichelli, Torino, 2007.
FIDELBO G., *Le Sezioni unite riconoscono rilevanza ai disturbi della personalità*, in *Cass. pen.*, 2005, p. 1850.
FILIPPI L., *L'intercettazione di comunicazioni*, Giuffrè, Milano, 1997.
FILIPPI L., *Commento all'art. 266 bis c.p.p.*, in A. GIARDA-G. SPANGHER (a cura di), *Codice di procedura penale commentato*, Ipsoa, Milano, 2007, p. 1921.
FIORI A., *La prova in medicina legale*, in *Riv. it. med. leg.*, 2004.
FIORI A., *Mito, realtà e fallacie del Dna (nella pratica forense)*, in *Riv. it. med. leg. (e dir. san.)*, 6, 2011, p. 1329.
FIORI A.-MARCHETTI D., *I garanti del sapere scientifico in sede giudiziaria*, in *Riv. it. med. leg.*, 33, 2011, p. 489.
FISHER G., *The Jury's Rise as Lie Detector*, in 107 *YALE L.J.*, 575, 1997.
FLOR R., *La Corte di giustizia considera la Direttiva europea 2006/24 sulla cd. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. e proc.*, 2009, 403.
FLORA M.G.P., *Biometria e clonazione delle impronte digitali*, in *Dir. Internet*, 2006, 6, p. 1 ss.
FLORIAN E., *Delle prove penali*, Cisalpino, Milano, 1961.
FLORIDI L., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina, Milano, 2014.
FLORIDI L., *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in *Philos. Technol.*, 34, 2021, p. 215-222.
FLORIDI L., *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Raffaello Cortina, Milano, 2022.
FLORIDI L.-HINE E., *The Blueprint for an AI Bill of Rights: In Search of Enaction, at Risk of Inaction*, in *Minds and Machines*, 33, 2023, p. 285-292.
FOCARDI F., *La consulenza tecnica extraperitale delle parti private*, Cedam, Padova, 2003.
FONSI A., *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time*, in *Riv. pen. dir. e proc.*, 13 maggio 2021.
FORMICI G., *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, in *Saggi-DPCE online*, 2, 2019.
FOSTER W.L., *Expert testimony. Prevalent complaints and proposed remedies*, in *Harvard L.R.*, 11, 1897, p. 169.

FOUCAULT M., *Surveiller et punir. Naissance de la prison*, Editions Gallimard, Paris, 1975.
FRANZEN J., *Purity*, Einaudi, Torino, 2016.
FRECKLETON J., *Problems posed by Dna evidence: of blood, babies and bathwater*, 17(1), in *Alternative Law Journal*, 10, 1992.
FREEMAN L., *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, in *Fordham International Law Journal*, Vol. 41, Issue 2, 2018, p. 283.
FRONZA E., CARUSO C., *Ti faresti giudicare da un algoritmo?, Intervista A. Garapon*, in *Quest. giust.* (web), 4, 2018, p. 196.
FURGIUELE A., *La prova per il giudizio nel processo penale*, Giappichelli, Torino, 2007.
FUSSEY P.-DAVIES B.-INNES M., *'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing*, in *The British Journal of Criminology*, 61(2), 2021.

GABRIELLI C., *"Accertamenti medici" dai confini troppo incerti*, in *Guida dir.*, 30, 2009, p. 73.
GABRIELLI C., *La decisione del "prelievo" torna al giudice*, in *Guida dir.*, 30, 2009, p. 68 ss.
GABRIELLI C., *Il prelievo coattivo di campioni biologici nel sistema penale*, Giappichelli, Torino, 2012.
GAITO A. (a cura di), *Studio sul processo penale in ricordo di Assunta Mazzarra*, Cedam, Padova, 1996.
GAITO A., *La prova penale*, Utet, Torino, 2008.
GALANTINI N., *L'inutilizzabilità della prova nel processo penale*, Cedam, Padova, 1992.
GALANTINI N., voce *Inutilizzabilità (dir. proc. pen.)*, in *Enc. dir.*, Agg. I, Milano, 1998, p. 648.
GALBALLY J.-FERRARA P.-HARAKSIM R.-PSYLLOS A.-BESLAY L., *Study on Face Identification Technology for its Implementation in the Schengen Information System*, *JRC*-34751, luglio 2019, p. 58.
GALBALLY J.-ROSS A.-GOMEZ-BARRERO M.-FIERREZ J.-ORTEGA-GARCIA J., *Iris Image Reconstruction from Binary Templates: An Efficient Probabilistic Approach Based on Genetic Algorithms*, in *Computer Vision and Image Understanding*, Vol. 117, Issue 10, October 2013, p. 1512-1525.
GALBOTTI S., *La libertà personale*, Giuffrè, Milano, 1953.
GALGANI B., *Habeas data e garanzie fondamentali*, in *Arch. pen. web.*, 1, 2019.
GALLO G., *Tecnologie di riconoscimento facciale e diritti fondamentali a rischio: il caso Glukhin c. Russia dinanzi alla Corte europea dei diritti dell'uomo*, in *Medialaws*, 3, 2024.
GALLUCCIO MEZIO G., *Il prelievo di materiale biologico dalla persona sottoposta*

a restrizione della libertà personale in una recente pronuncia della Corte Suprema degli Stati Uniti, in *Cass. pen.*, 5, 2014, p. 1874.
GALTON F., *Biometry*, in *Biometrika*, Vol. 1, Issue 1, October 1901, p. 7-10.
GARAPON A.-LASSÉGUE J., *La giustizia digitale. Determinismo tecnologico e libertà*, il Mulino, Bologna, 2021.
GARBOLINO P., *Nuovi strumenti logici e informatici per il ragionamento giudiziario: le reti bayesiane*, in *Cass. pen.*, 2007, p. 326.
GARBOLINO P., *Probabilità e logica della prova*, Giuffrè, Milano, 2014.
GARGANI A., *I rischi e le possibilità dell'applicazione dell'analisi del Dna nel settore giudiziario*, in *Riv. it. dir. proc. pen.*, 1993, p. 1310.
GARRET L., *Judging Innocence*, in *Columbia Law Review*, 108, 2008, p. 55 ss.
GARVIE C., *Garbage In, Garbage Out: Face Recognition on Flawed Data*, in *Georgetown Law, Center on Privacy and Technology*, 16 maggio 2019.
GARVIE C.-BEDOYA A.-FRANKLE J., *The perpetual line-up: Unregulated police face recognition in America*, in *Georgetown Law, Center on Privacy & Technology*, reperibile su https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%201216 16.pdf.
GATES K.A., *Our Biometric Future. Facial recognition technology and the culture of surveillance*, New York University Press, New York, 2011.
GENNARI G., *Bioinformazione e indagini penali: la l. 85 del 30 giugno 2009*, in *Resp. civ.*, 12, 2009, p. 2630B.
GERACI R.M., *La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento E-evidence*, in *Cass. pen.*, 2019, p. 1340 ss.
GERADTS Z.-FRANKE K. (eds.), *Artificial Intelligence (AI) in Forensic Sciences*, John Wiley & Sons Inc, Hoboken, 2023.
GERRA G., *Alcune tecniche di identificazione biometrica di pratica attuabilità*, in *Riv. giur. sarda*, 2001.
GIALUZ M., *Radiologia e accertamenti medici coattivi: il difficile equilibrio tra libertà della persona ed esigenze di prova*, in *Riv. it. dir. proc. pen.*, 2, 2012, p. 558-579.
GIALUZ M., *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *Dir. pen. cont. online*, 29 maggio 2019.
GIALUZ M., *L'emergenza nell'emergenza: il decreto-legge n. 28 del 2020, tra ennesima proroga delle intercettazioni, norme manifesto e "terzo tempo" parlamentare*, in *Sist. pen.*, 1 maggio 2020.
GIALUZ M., *Premessa*, in *Diritto di Internet, digital copyright and data protection*, suppl. 3, 2020.
GIALUZ M., *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Giuffrè, Milano, 2021, p. 51-68.

GIALUZ M.-DELLA TORRE J., *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir. pen. cont.*, 5, 2018, p. 277 ss.
GIANFORMAGGIO L.-LECALDANO E. (a cura di), *Etica e diritto. Le vie della giustificazione razionale*, Laterza, Roma-Bari, 1986.
GIANNELLI P.C., *The abuse of scientific evidence of criminal cases: the need for independent laboratories*, in *Virginia J. Social Policy & Law*, 4, 1997, p. 439 ss.
GIANNINI A.M.-TIZZANI E.-D'AMORE A., *L'identikit: come si aiuta un testimone a ricordare*, in *Rass. it. crimin.*, 4, 2012.
GILLESPIE T.-BOCZKOWKI P.-FOOT K., *Media Technologies. Essays on Communication, Materiality, and Society*, The MIT Press, Cambridge, 2014.
GIOSTRA G., voce *Contraddittorio (principio del)*, in *Enc. giur.*, VIII, Roma, 1988.
GIOSTRA G., *Analisi e prospettive di un modello incompiuto*, in *Quest. giust.*, 2001, p. 1130.
GIOSTRA G., *Gli importanti meriti e i molti limiti della nuova disciplina*, in *Giur. it.*, 2010, p. 1219 ss.
GIOSTRA G.-ORLANDI R. (a cura di), *Nuove norme in materia di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Giappichelli, Torino, 2018.
GIROTTO S., *Biometria e nanomedicina: le nuove frontiere della riconcettualizzazione tecnologica del corpo umano*, in *Nuova giur. civ.*, 9, 2009, 20452.
GIROTTO S., *Trattamento di dati biometrici e dignità della persona*, in *Nuova giur. civ. comm.*, 3, 2012, p. 242 ss.
GIULIANI A., *Il concetto di prova. Contributo alla logica giuridica*, Giuffrè, Milano, 1961.
GIULIANI A., voce *Prova (filosofia)*, in *Enc. dir.*, XXXVII, Milano, 1988, p. 518.
GIULIANO A., *Dal pensiero di Lombroso all'impronta digitale. Passato e presente del metodo più efficiente, pratico e rapido d'identificazione personale*, Edizioni libreria Cortina, Torino, 2012.
GIUNCHEDI F., *Gli accertamenti tecnici irripetibili*, Giappichelli, Torino, 2009.
GIUNCHEDI F., *Le malpractices nella digital forensics. Quali conseguenze sull'inutilizzabilità del dato informatico?*, in *Arch. pen.*, 3, 2013, p. 861 ss.
GIUNTA F., *Questioni scientifiche e prova scientifica tra categoria sostanziale e regole di giudizio*, in *Criminalia*, 2014.
GIUSTOZZI C., *Giuristi e informatici divisi da una lingua comune: autenticazione?*, reperibile su http://www.interlex.it/forum10/relazioni/24giustozzi.htm.
GRAND J.S., *The blooding of America: Privacy and the Dna Dragnet*, in *23 Cardozo L. Rev.*, 2002, p. 2277.
GRANJA R.-AMORIM A., *Ethical challenges of merging criminal identification and*

civil identification within the Prüm system, in *Forensic Science International: Genetics*, 57, 2022.
GRECO L.-MANTELERO A., *Industria 4.0, robotica e privacy-by-design*, in *Dir. inf. e inform.*, 6, 1 dicembre 2018, 875.
GREENLEAF G., *Renewing Convention 108: The CoÈs 'GDPR Lite' Initiatives*, 142 *Privacy Laws & Business International Report*, 14-17 agosto 2016.
GREENWOOD V., *Sulla scena del crimine. Le nuove frontiere delle scienze forensi*, in *National Geographic*, 38(1), luglio 2016.
GREVI V., *Nemo tenetur se detegere: interrogatorio dell'imputato e diritto al silenzio nel penale italiano*, Giuffrè, Milano, 1972.
GREVI V., voce *Libertà personale dell'imputato*, in *Enc. dir.*, XXIV, Giuffrè, Milano, 1974.
GREVI V., *Libertà personale e Costituzione*, Giuffrè, Milano, 1976.
GREVI V. (a cura di), *La libertà personale dell'imputato. Verso il nuovo processo penale*, Cedam, Padova, 1989.
GREVI V., *Alla ricerca di un processo penale giusto*, Giuffrè, Milano, 2000.
GRIFANTINI F.M., voce *Inutilizzabilità*, in *Dig. disc. pen.*, III, Utet, Torino, 1993.
GRIFANTINI F.M., *Il segreto difensivo nel processo penale*, Giappichelli, Torino, 2001.
GRIFANTINI F.M., *La nozione di indizio nel codice di procedura penale*, in *Riv. dir. proc.*, 1, 2013, p. 12.
GRIJPINK J., *Privacy Law: Biometrics and Privacy*, in *CL&SR*, (2001) 17(3), 154, p. 156-157 ss.
GROTHER P.-NGAN M.-HANAOKA K., *Face Recognition Vendor Test (FRVT). Part 2: Identification*, in *NIST*, dicembre 2020.
GUALTIERI P., *Prova informatica e diritto di difesa*, in *Dir. pen. e proc.*, 2008.
GUARRIELLO V., *L'intelligenza artificiale tra profili giuridici ed alcune delle più attuali applicazioni al servizio della società*, reperibile su https://arsg.it/?p=1781.
GULOTTA G., *Psicologia della testimonianza*, in AA.VV., *Trattato di psicologia giudiziaria nel sistema penale*, a cura di G. GULOTTA, vol. I, Giuffrè, Milano, 1987, p. 499 ss.
GULOTTA G.-TUOSTO E.M., *Il volto nell'investigazione e nel processo. Nuova fisiognomica forense*, Giuffrè, Milano, 2017.
GUO G.-MU G.-RICANEK K., *Cross-age face recognition on a very large database: the performance versus age intervals and improvement using soft biometric traits*, in *Proc. 20th Int. Conf. Pattern Recognit.*, Aug. 2010, p. 3392-3395.

HAACK S., *Legalizzare l'epistemologia. Prova, probabilità e causa nel diritto*, Università Bocconi, Milano, 2015.
HACKER P., *Comments on the Final Trilogue Version of the AI Act*, reperibile su https://www.europeannewschool.eu/images/chairs/hacker/Comments%20on%20the%20AI%20Act.pdf.

HANSEN P.B., *Classic Operating Systems: From Batch Processing to Distributed Systems*, Springer, New York, 2001.
HARLEY J.M., *Measuring Emotions: A Survey of Cutting Edge Methodologies Used in Computer-Based Learning Environment Research*, in S.Y. TETTEGAH-M. GARTMEIER (eds.), *Emotions, Technology, Design, and Learning*, Elsevier Academic Press, Cambridge, 2016.
HARS A., *Conceptual Difficulties in the Transformation of Human Rights to the Realm of Artificial Intelligence*, in *Acta Humana*, 2, 2024.
HÉNIN S., *AI. Intelligenza artificiale tra incubo e sogno*, Hoepli, Milano, 2019.
HILDEBRANDT M., *The Proposal for an EU AI Act of 21 April 2021*, *Brief Commentary*, 2021, reperibile su https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legalrequirements/F2662611_en.
HILDEBRANDT M.-DE VRIES K., *Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology*, Routledge, Abingdon, 2013.
HILL K. (trad. V. Parodi), *La tua faccia ci appartiene*, Garzanti, Milano, 2024.
HOUSSEIN E.H.-HAMMAD A.-ALI A.A., *Human emotion recognition from EEG-based brain–computer interface using machine learning: a comprehensive review*, in *Neural Comput & Applic*, 34, 2022, p. 12527-12557.
HRICK P.-HEYDARI F., *The Growing World of Face Recognition Legislation: A Guide to Enacted and Proposed Legislation*, reperibile su https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5d9f7965391b2358bdccda63/1570732405589/The+Growing+World+of+Face+Recognition+Legislation.pdf.
HUBER P.W., *Galileo's revenge. Junk science in the Courtroom*, Basic books, New York, 1993.
HUTCHINS B.-ANDREJEVCIC M., *Olympian Surveillance: Sports Stadiums and the Normalization of Biometric Monitoring*, in *International Journal of Communication*, 15, 2021, p. 363-382.
HWANG H.-MATSUMOTO D., *Evidence for the universality of facial expressions of emotion*, in M.K. MANDAL-A. AWASTHI, *Understanding facial expressions in communication: Cross-cultural and multidisciplinary perspectives*, 2015, p. 41-56.

IACONO W.G.-LYKKEN D.T., *The validity of the lie detector: Two surveys of scientific opinion*, in *Journ. of Appl. Psychol.*, 82(3), 1997, p. 426-433.
IANNUZZI A., *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Editoriale Scientifica, Napoli, 2018.
IANNUZZI A.-FILOSA F., *Il trattamento dei dati genetici e biometrici*, in *Dirittifondamentali.it*, 2, 2019.
IASELLI M. (a cura di), *Investigazioni digitali*, Giuffrè, Milano, 2020.

IENCA M., *Intelligenza². Per un'unione di intelligenza naturale e artificiale*, Rosenberg & Sellier, Torino, 2019.
INTINI A.-CASTO A.R.-SCALI D.A., *Investigazione di polizia giudiziaria. Manuale delle tecniche investigative*, Laurus Robuffo, Roma, 2006.
INTRONA F.-RAGO C.-REGAZZO A., *Il giudice e il coraggio del dubbio*, in *Riv. it. med. leg.*, 1997, p. 447 ss.
IOVANE G.-MAGRO G., *STUDI-La biometria e nuovi sistemi di identificazione*, in *Rass. Arma Carab.*, luglio-settembre 2004, suppl. al n. 4.

JACQUET M.-CHAMPOD C., *Automated face recognition in forensic science: Review and perspectives*, in *Forensic Science International*, 307, 2020, p. 1-14.
JAFRI R.-ARABNIA H.R., *A survey of face recognition techniques*, in *Journal of Information Processing Systems*, 5, 2009, p. 41-68.
JAIN A.K., *Biometrics: Past, Present and Future*, in *18th IAPR/IEEE Int.l Summer school for advanced studies on biometrics: BIOMETRICS FOR AI / AI FOR BIOMETRICS*, May 30-June 4,2021.
JAIN A.K.-PANKANTI S., *Biometrics Systems: Anatomy of Performance*, in *IEICE TRANS. FUNDAMENTALS*, Vol. E00-A, NO, 2001.
JAIN A.K.-ROSS A., *Bridging the Gap: From Biometrics to Forensics*, in *Philosophical Transactions of the Royal Society*, 2015, disponibile su http://rstb.royalsocietypublishing.org/content/370/1674/20140254.
JAIN A.K.-BOLLE R.-PANKANTI S., *Biometrics. Personal identification in Networked Society*, Kluwer Academic Publishers, Norwell, 1999.
JAIN A.K.-DEB D.-ENGELSMA J.J., *Biometrics: Trust, but Verify*, su https://arxiv.org/abs/2105.06625, 14 May 2021.
JAIN A.K.-NANDAKUMAR K.-ROSS A., *50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities*, 2016, in http://biometrics.cse.msu.edu/pubs/gen_biometrics.html.
JAIN A.K.-ROSS A.-NANDAKUMAR K., *Introduction to biometrics: a textbook*, Springer, Berlino, 2011.
JAIN A.K.-ROSS A.-PRABHAKAR S., *An Introduction to Biometric recognition*, in *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 2004, p. 4-20.
JAIN A.K.-PANKANTI S.-PRABHAKAR S.-HONG L.-ROSS A.-WAYMAN J.L., *Biometrics: A Grand Challenge, Proceedings of International Conference on Pattern Recognition*, Cambridge, UK, Aug. 2004, http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/Jainetal_BiometricsGrandChallenge_ICPR04.pdf.
JAKCSON J.-LANGER M.-TILLERS P. (eds.), *Crime, Procedure and Evidence in a Comparative and International Context. Essays in Honour of Professor Mirjan Damaŝka*, Hart Publishing, Oxford-Portland, 2008.

JASANOFF S., *La scienza davanti ai giudici. La regolazione giuridica della scienza in America*, Giuffrè, Milano, 2001.
JASSERAND C., *Avoiding terminological confusion between the notions of 'biometrics' and 'biometric data': an investigation into the meanings of the terms from a European data protection and a scientific perspective*, in *International Data Privacy Law*, 6(1), 2016.
JASSERAND C., *Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data*, in *EDPLR*, 2(3), 2016, p. 297-311.
JASSERAND C., *New Extensive Guidelines on the Use of Facial Recognition by the Council of Europe*, in *EAB's Newsletter*, 2021.
JASWAL G.-KANHANGAD V.-RAMACHANDRA R. (eds.), *AI and Deep Learning in Biometric Security*, CRC Press, Boca Raton, 2021.
JEFFREYS A.J.-WILSON V.-THEIN S.L., *Individual-Specific 'Fingerprints' of Human DNA*, in *Nature*, 316, 1985.

KAK A. (a cura di), *Regulating Biometrics: Global Approaches and Urgent Questions*, in *AI Now Institute*, 2020.
KALB L., *Il documento nel sistema probatorio*, Giappichelli, Torino, 2000.
KALB L. (a cura di), *Diritti della persona e nuove sfide del processo penale*, Giuffrè, Milano, 2019.
KAMINSKI M.E.-MALGIERI G., *The Right to Explanation in the AI Act*, in *U of Colorado Law Legal Studies Research Paper*, No. 25-9, 2025.
KAPLAN J., *Intelligenza artificiale. Guida al futuro prossimo*, Luiss, Roma, 2017.
KAUBA C.-KIRCHGASSER S.-MIRJALILI V.-UHL A.-ROSS A., *Inverse Biometrics: Generating Vascular Images from Binary Templates*, in *IEEE Transactions on Biometrics, Behavior, and Identity Science* (T-BIOM), 2021.
KAUR H.-KHANNA P., *Biometric template protection using cancelable biometrics and visual cryptography techniques*, in *Multimed Tools Appl*, 75, 2016, p. 16333-16361.
KAUR P.-KRISHAN K.-SHARMA S.K.-KANCHAN T., *Facial-recognition algorithms: a literature review*, in *Medicine, Science and the Law*, 60(2), 2020, p. 131-139.
KAYE D.H., *Statistics for lawyers and law for statistics*, in 89 *Mich. L. Rev.*, 1991, p. 1520.
KAYE D.H., *A Fourth Amendament Theory for Arrestee Dna and other Biometric Databases*, in *Univ. of Pennsylv. Journ. of Const. Law*, 15(4), 2013, p. 1095-1160.
KEENAN B., *Automatic Facial Recognition and the Intensification of Police Surveillance*, in *Modern Law Review*, 84(4), 2021, p. 886-897.
KENNEDY R., *Algorithms and the Rule of Law*, in *Computers and Law*, aprile/maggio 2017, p. 23 ss.
KERR O., *Digital Evidence and the New Criminal Procedure*, in 105 *Columbia Law Review*, 2005.

KHAIRWA A.-ABHISHEK K.-PRAKASH S.-PRATAP T., *A comprehensive study of various biometric identification techniques*, in 2012 *Third International Conference on Computing, Communication and Networking Technologies* (ICCCNT' 12), 2012, p. 1-6.

KHAN A.Z.-RIZVI A., *AI based facial recognition technology and criminal justice: issues and challenges*, in *Turkish Journal of Computer and Mathematics Education*, 12(14), 2021, p. 3384-3392.

KHELIF K. *et al.*, *Towards a Breakthrough Speaker Identification Approach for Law Enforcement Agencies: SIIP*, in *2017 European Intelligence and Security Informatics Conference (EISIC)*, 2017, p. 32-39.

KHUN T.S., *La struttura delle rivoluzioni scientifiche. Come mutano le idee della scienza*, Einaudi, Torino, 1999.

KIM B.-KHANNA R.-KOYEJO O.O., *Examples are not enough, learn to criticize! Criticism for interpretability*, in *Advances in Neural Information Processing Systems*, MIT Press: Cambridge, MA, 2016, p. 2280 ss.

KIND C., *Containing the canary in the AI coalmine – the EU's efforts to regulate biometrics*, in *Ada Lovelace Institute*, 2021, reperibile su https://www.adalovelaceinstitute.org/blog/canary-ai-coalmine-eu-regulate-biometrics/.

KINDT E.S., *Having yes, using no? About the new legal regime for biometric data*, in *Comp. Law and Sec. Rev.*, 34, 2018, p. 523-538.

KITCHIN R., *The real-time city? Big data and smart urbanism*, in *GeoJournal*, 79, 2014, p. 1-14.

KITCHIN R., *Thinking critically about and researching algorithms*, in *Information, Communication and Society*, 20(1), 2017, p. 1-14.

KLEINBERG K.F.-PHARM B.-VANEZIS P.M.D.-BURTON A.M., *Failure of Anthropometry as a Facial Identification Technique Using High-Quality Photographs*, in *Journal of Forensic Sciences*, 52(4), 2007, p. 779-783.

KOEHLER J.J.-CHIA A.-LINDSEY S., *The random match probability in Dna evidence: irrelevant and Prejudicial*, in *Jurimetrics Journal*, 1995, p. 201-218.

KOMARINSKI P., *Automated fingerprint identification systems* (AFIS), Elsevier Academic, Amsterdam, 2005.

KOOPS B.J.-NEWELL B.C.-TIMAN T.-SKORVANEK I.-CHOKREVSKI T.-GALIC M., *A typology of privacy*, in *Univ. of Pennsyl. Journ. of Intern. Law*, 2017.

KORTYLEWSKI A.-EGGER B.-SCHNEIDER A.-GERIG T.-MOREL-FORSTER A.-VETTER T., *Analyzing and Reducing the Damage of Dataset Bias to Face Recognition With Synthetic Data*, in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, 2019, p. 1-8.

KOSTORIS R.E., *I consulenti tecnici nel processo penale*, Giuffrè, Milano, 1993.

KOSTORIS R.E., *Alt ai prelievi di sangue coattivi*, in *Dir. pen. e proc.*, 1996, p. 1094 ss.

KOSTORIS R.E., *La lotta al terrorismo e alla criminalità organizzata tra speciali*

misure processuali e tutela dei diritti fondamentali nella Risoluzione del XVIII Congresso internazionale di diritto penale, in *Riv. dir. proc.*, 2010.

KOSTORIS R.E., *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, in F. RUGGIERI-L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica*, Giappichelli, Torino, 2011.

KOSTORIS R.E.-ORLANDI R. (a cura di), *Contrasto al terrorismo interno e internazionale*, Giappichelli, Torino, 2006.

KRAUSOVÁ A., *Intersections between Law and Artificial Intelligence*, in *Int. Jour. of Comp. (IJC)*, 27(1), 2017, p. 55-68.

KROLL J.A.-HUEY J.-BAROCAS S.-FELTEN E.W.-REIDENBERG J.R.-ROBINSON D.G.-HARLAN YU, *Accountable Algorithms*, in 165 *U. Pa. L. Rev.*, 633, 2017.

KUMAR A.-KAUR N., *Face Recognition*, in *International Journal of Advanced Trends in Computer Applications (IJATCA)*, 3(2), February 2016, p. 10-15.

LABATE MANTOVANINI PADUA LIMA M.L. GARCEZ-GHIRARDI J. (eds.), *Global Law. Legal Answers for Concrete Challenges*, Juruà Editorial, Porto, 2018.

LA CAVA S.M.-ORRÙ G.-DRAHANSKY M.-MARCIALIS G.-ROLI F., *3D Face Reconstruction: The Road to Forensics*, in *ACM Comput. Surv.*, 56, 3, 2023, Article 77, 77:8.

LAGO G., *Banche dati del Dna: raccomandazioni internazionali, studio comparato con la Legge 85/2009*, in *Giust. pen.*, 2010, p. 141 ss.

LA MUSCATELLA D., *Il trattamento della prova digitale nel sistema processuale penale italiano. Anamnesi e prognosi di una patologia classica, declinata in una (apparente) riforma*, in *Informatica e diritto*, anno XLI, vol. XXIV, n. 1-2, 2015, p. 263-279.

LA REGINA K., *L'identificazione della voce nel processo penale*, reperibile su https://www.letture.org/l-identificazione-della-voce-nel-processo-penale-katia-la-regina.

LA REGINA K., *L'identificazione della voce nel processo penale*, Wolters Kluwer Cedam, Milano, 2018.

LA REGINA K., *Riconoscimento della voce – brevi note sul riconoscimento della voce nel processo penale*, in *Giur. it.*, 1, 2018, p. 212.

LA ROCCA E.N., voce *Inutilizzabilità*, in *Dig. disc. pen.*, Agg. I, Torino, 2008, p. 613 ss.

LARONGA A., *Il pedinamento satellitare: un atto atipico lesivo di diritti inviolabili?*, in *Quest. giust.*, 2002, p. 1153.

LASAGNI G., *Tackling phone searches in Italy and the United States: Proposals for a technological rethinking of procedural rights and freedoms*, in *New Journal of European Criminal Law*, 2018, p. 38-401.

LASAGNI G., *Difendersi dall'intelligenza artificiale o difendersi con l'intelligenza artificiale? Verso un cambio di paradigma*, in *Riv. it. dir. e proc. pen.*, 4, 2022, p. 1545.

LAVANYA B.-INBARANI H.H., *A Survey of Biometric Techniques*, in *International*

Journal of Advanced Research in Computer Science and Software Engineering, Vol. 5, Issue 7, 2015.

LAVARINI B., *Elementi di procedura penale. Lezioni per il corso di laurea magistrale in chimica clinica, forense e dello sport*, Ecig Universitas, Genova, 2010.

LAVORGNA A.-SUFFIA G., *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale*, in *Dir. pen. cont.-Riv. trim.*, 2, 2021, p. 88 ss.

LEE Y.-FILLIBEN J.J.-MICHEALS R.J.-PHILLIPS P.J., *Sensitivity analysis for biometric systems: A methodology based on orthogonal experiment designs*, in *Computer Vision and Image Understanding*, 117(5), 2013, p. 532-550.

LEENES R.-DE CONCA S., *Artificial intelligence and privacy. Ai enters the house through the cloud*, in W. BARFIELD-U. PAGALLO (eds.), *Research Handbook on the Law of Artificial Intelligence*, Edward Elgar publishing, Cheltenham-Northampton, 2018, p. 295.

LENGKONG O.H.-TAJU S.-MAABUAT C.F.-JANIS R.J., *Security System To Prevent Terrorism Actions Using Face Recognition*, in *Worship Building, 2023 5th International Conference on Cybernetics and Intelligent System* (ICORIS), 2023, p. 1-6.

LEO W., *What are the Effects of the Daubert Decision on Fingerprint Identification?*, disponibile su http://www.fingerprintidentification.net/sitebuilder-content/sitebuilderfiles/researchpaperondaubert1.pdf.

LESLIE D., *Understanding bias in facial recognition technologies*, in *The Alan Turing Institute*, 2020.

LEVANTINO F.P.-PAOLUCCI F., *Advancing The Protection Of Fundamental Rights Through AI Regulation: How The Eu And The Council Of Europe Are Shaping The Future*, in *SSRN*, 2024, p. 1-16.

LEVANTINO F.P.-REZENDE I.N., *Rischio inaccettabile: usi proibiti*, in O. POLLICINO-F. DONATI-G. FINOCCHIARO-F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, Giuffrè, Milano, 2025.

LEYS R., *How Did Fear Become a Scientific Object and What Kind of Object Is It?*, in *Representations*, 110(1), 2010, p. 66-104.

LI S.Z.-JAIN A.K. (a cura di), *The Handbook of Face Recognition*, Springer, New York, 2011.

LI S.Z.-JAIN A.K., *Encyclopedia of Biometrics*, Springer, Boston, 2015.

LIANG F.-DAS V.-KOSTYUK N.-HUSSAIN M.M., *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, in *Policy and Internet*, 4(10), 2018, p. 415 ss.

LIEBMAN J.S.-RIFKIND S.H.-FAGAN J.-WEST V., *A broken system: errors in capital causes 1973-1995*, Columbia University, 2000, http://www2.law.columbia.edu/instructionalservices/liebman/liebman_final.pdf.

LINARELLO P., *La banca dati nazionale del Dna*, in *Il Penalista*, 14 marzo 2016, http://ilpenalista.it/articoli/indagini-scientifiche/la-banca-dati-nazionale-del-dna.

LINSKY L. (a cura di), *Semantica e filosofia del linguaggio*, Giuffrè, Milano, 1969.
LIPTON Z.C., *The mythos of model interpretability*, in *arXiv*, 2016.
LOMBARDO L., *La scienza e il giudice nella ricostruzione giudiziale del fatto*, in *Riv. dir. proc.*, 2007, 35.
LOPEZ R., *Videosorveglianza biometrica tramite riconoscimento facciale: parere negativo del Garante per la privacy*, in *Proc. pen. e giust.*, 2022, p. 798 ss.
LORUSSO S. (a cura di), *Le nuove norme sulla sicurezza pubblica*, Cedam, Padova, 2008.
LORUSSO S. (a cura di), *Prova penale e metodo scientifico*, Utet, Torino, 2009.
LORUSSO S., *Il contributo degli esperti alla formazione del convincimento giudiziale*, in *Arch. pen.*, 2011, p. 809 ss.
LORUSSO S., *L'esame della scena del crimine nella contesa processuale*, in *Dir. pen. e proc.*, 2011.
LOZZI G., *Lezioni di procedura penale*, Giappichelli, Torino, 2013.
LUCARELLI A.-PICOZZI M., *Tracce criminali. Storie di omicidi imperfetti*, Mondadori, Milano, 2006.
LUIS GARCIA R.D.-ALBEROLA LOPEZ C.-AGHZOUT O.-RUIZ-ALZOLA J., *Biometric identification systems*, in *Signal Processing*, 83(12), 2003, p. 2539-2557.
LUPARIA L., *I profili processuali*, in *Dir. pen. e proc.*, 2008.
LUPARIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48*, in *Dir. pen. e proc.*, 2008.
LUPARIA L. (a cura di), *Sistema penale e criminalità informatica*, Giuffrè, Milano, 2009.
LUPARIA L., *Computer crimes e procedimento penale*, in G. GARUTI (a cura di), *Trattato di procedura penale. Modelli differenziati di accertamento*, Utet giuridica, Torino, 2011.
LUPARIA L., *Note conclusive nell'orizzonte d'attuazione dell'Ordine europeo di indagine*, in T. BENE-L. LUPARIA-L. MARAFIOTI (a cura di), *L'ordine europeo di indagine. Criticità e prospettive*, Giappichelli, Torino, 2016, p. 249 ss.
LUPÀRIA L., *Privacy, diritti della persona e processo penale*, in *Riv. dir. proc.*, 6, 2019, p. 1449.
LUPARIA L.-ZICCARDI G., *Investigazione penale e tecnologia informatica*, Giuffrè, Milano, 2007.
LYON L., *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2002.
LYON V.D., *Massima sicurezza. Sorveglianza e «guerra al terrorismo»*, Raffaello Cortina, Milano, 2005.

MAGGINO F.-CICERCHIA G., *Algoritmi, etica e diritto*, in *Dir. inf. e inform.*, 6, 1 dicembre 2019, p. 1161.
MAGNANI G.A.-FERRETTI G.-ROCCO P., *Tecnologie dei sistemi di controllo*, McGraw-Hill, New York, 2011.

MAI G.-CAO K.-PONG C. YUEN-JAIN A.K., *On The Reconstruction Of Face Images From Deep Face Templates*, in the *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2018.

MAIO D.-MALTONI D.-CAPPELLI R.-WAYMAN J.L.-JAIN A.K., *FVC2002: Fingerprint verification competition*, in *Proc. Int. Conf. Patt. Rec. (ICPR)*, Quebec City, QC, Canada, Aug. 2002, p. 744-747.

MAIOLI C., *Dar voce alle prove: elementi di informatica forense, in Crimine virtuale, minaccia reale*, Franco Angeli, Milano, 2004.

MAIOLI C. (a cura di), *Questioni di informatica forense*, Aracne, Roma, 2015.

MALGIERI G.-COMANDÈ G., *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 7(2), 2017.

MANES V., *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *DisCrimen*, 15 maggio 2020.

MANFREDI V.-PESSA E., *Il riconoscimento dei volti: aspetti cognitivi, neuropsicologici e computazionali*, in *Sist. intell.*, 3, 2011.

MANGIARACINA A., *Il riconoscimento facciale: nuove sfide nel processo penale*, in P. DI SIMONE-A. MANGIARACINA-L. PARLATO (a cura di), *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, Palermo University Press, Palermo, 2023.

MANTELERO A., *La gestione del rischio*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, Zanichelli, Bologna, 2019.

MANTELERO A., *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template*, in *Computer Law & Security Review*, 54, 2024.

MARAFIOTI L., *Digital evidence* e processo penale, in *Cass. pen.*, 2011, p. 4509-4523.

MARAFIOTI L.-LUPARIA L. (a cura di), *Banca dati del Dna e accertamento penale*, Giuffrè, Milano, 2010.

MARANDOLA A., *Il riconoscimento facciale*, in C. CONTI-A. MARANDOLA (a cura di), *La prova scientifica*, Giuffrè, Milano, 2023, p. 495-510.

MARCHESE V.-CAENAZZO L.-RODRIGUEZ D., *Banca dati nazionale del Dna: bilanciamento tra diritti individuali e sicurezza pubblica nella legge 30 giugno 2009, n. 85*, in *Riv. it. dir. e proc. pen.*, 4, 2013, p. 1863.

MARCHETTI D.-SOLECCHI G.-CASCINI F.-ALBERTACCI G., *Il valore probatorio dell'immagine digitale*, in *Giust. pen.*, I, 2004, c. 276.

MARCOLINI S., *Regole di esclusione e nuove tecnologie*, in *Criminalia*, 1, 2006.

MARCOLINI S., *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2, 2015, p. 761.

MARI A., *Sub art. 359*, in G. LATTANZI-E. LUPO (a cura di), *Codice di procedura penale. Rassegna di giurisprudenza e dottrina*, vol. V, Giuffrè, Milano, 2017.

MARIN L.-MONTALDO S., *The Fight Against Impunity in EU Law*, Hart Publishing, New York, 2020.
MARINO G., *Individuazione e prelievo di reperti utili per la ricerca del DNA: la Costituzione impone il contraddittorio?*, in *Dir. & giust.*, 183, 2017.
MARTURANO A., *Il corpo Digitale: natura, informazione, merce*, Giappichelli, Torino, 2010.
MASON S., *Electronic Evidence: Disclosure, Discovery and Admissibility*, LexisNexis, Londra, 2007
MASSA T., *Le Sezioni unite davanti a "nuvole e orologi": osservazioni sparse intorno al principio di causalità*, in *Cass. pen.*, 2002, p. 3643.
MASTROIANNI R.-POLLICINO O.-ALLEGREZZA S.-PAPPALARDO F.-RAZZOLINI O. (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, Milano, 2017.
MASTROPAOLO F., *Prelievi del sangue a scopo probatorio e poteri del giudice*, in *Riv. it. med. leg.*, 9, 1987, p. 1081.
MATHER K., *Elementi di biometria*, in *Testi e manuali per la scienza contemporanea. Serie di biologia e medicina*, Boringheri, Torino, 1972.
MATTIUCCI M.-DELFINIS G., *Forensic Computing*, in *Rass. Arma Carab.*, 2, 2006, p. 51 ss.
MAZZA O. (a cura di), *Le nuove intercettazioni*, Giappichelli, Torino, 2018.
MAZZA O., *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Dir. pen. cont.-Riv. trim.*, 3, 2019.
MAZZACUVA N.-PAPPALARDO G., *Prelievo ematico coattivo e accertamento della verità: spunti problematici*, in *Foro it.*, 1987, I, c. 717 ss.
MCCARTNEY C., *The Dna expansion programme and criminal investigation*, in *Brit. J. Criminol.*, 46, 2006, p. 175-192.
MCCONVEY J.R., *Does facial recognition work if surgery alters a person's face? Reconstructive and cosmetic changes to facial geometry pose challenges for biometrics*, in *Biometricupdate*, 10 aprile 2024.
MCEWAN I., *Macchine come me*, Einaudi, Torino, 2019.
MCSTAY A., *Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy*, in *Big Data & Society*, 2020.
MECHAM L.R., *Il sistema giudiziario federale negli Stati Uniti. Elementi introduttivi per i magistrati e gli amministratori giudiziari in altri paesi*, Washington D.C. 20544, 2001, disponibile su http://pub.raffaelecassia.it/sss/eclipse/legal_usa.pdf.
MELCHIONDA A., voce *Prova in generale (dir. proc. pen.)*, in *Enc. dir.* XXXVIII, Milano, 1988.
MENDOLA M., *Aspetti informatici delle prove biometriche. Il problema dei "falsi positivi"*, in *Psicologia e Giustizia*, anno 14, n. 1, gennaio-giugno 2013.
MENÉNDEZ N.-MOBILIO G., *Between prohibited risks and high risks: the regulation of facial recognition technology*, in O. POLLICINO-F. DONATI-G. FINOC-

CHIARO-F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, Giuffrè, Milano, 2025.

MENÉNDEZ N.-MOBILIO G., *Next Democratic Frontiers for Facial Recognition Technology (FRT). The Legal, Ethical and Democratic Implications of FRT*, Springer, Cham, 2025.

MENNA M., *La prova tra processo, scienza e verità. Quel rapporto giudice accertamento*, in *Dir. & giust.*, 19, 2006, p. 95.

MEUWLY D.-BAKER N., *Biometrics in the aliens' identity chain. A literature study final report* (WODC PROJECT 2965), reperibile su https://repository.wodc.nl/bitstream/handle/20.500.12832/2428/2965_volledige_tekst_tcm28-442367.pdf?sequence=3&isAllowed=y.

MEUWLY D.-RAMOS D.-HARAKSIM R., *A guideline for the validation of likelihood ratio methods used for forensic evidence evaluation*, in *Forensic Science International*, 276, 2017, p. 142-153.

MILANI S.-FONTANI M.-BESTAGINI P.-BARNI M.-PIVA A.-TAGLIASACCHI M.-TUBARO S., *An overview on video forensic*, in *APSIPA Transactions on Signal and Information Processing*, 1, 2012.

MILLER T., *Explanation in Artificial Intelligence: Insights from the social sciences*, in *Artif. Intell.*, 267, 2018, p. 1-38.

MIRAGLIA M., *Il IV Emendamento alla rincorsa del progresso: perquisizioni e lotta alla droga nel diritto Usa*, in *Dir. pen. e proc.*, 2002, p. 105 ss.

MIRAGLIA M., *La ricerca della verità per condannare ed assolvere: il test del Dna e l'esperienza statunitense*, in *Dir. pen. e proc.*, 12, 2003, p. 1555.

MITTELSTADT B.-FLORIDI L., *The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts*, in *Science and Engineering Ethics*, 22, 2016, p. 303 ss.

MITTONE A., *Libero convincimento e sapere scientifico: riflessioni sulla perizia nel processo penale*, in *Quest. giust.*, 1983.

MNOOKIN J.L., *The validity of latent fingerprint identification: confessions of a fingerprinting moderate*, in *Law, Probability and Risk*, 7, 2008, p. 127-141, si veda https://lpr.oxfordjournals.org/content/7/2/127.full.pdf.

MOBILIO G., *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, in *Federalismi.it*, 16, 2020.

MOBILIO G., *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli, 2021.

MOBILIO G., *L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?*, in E. DI CARPEGNA BRIVIO-A. SANCINO (a cura di), *La democrazia della società digitale. Tensioni e opportunità. Atti del Convegno 3 dicembre 2021*, Università di Milano-Bicocca, 2023.

MOBILIO G., *Your face is not new to me – Regulating the surveillance power of facial recognition technologies*, in *Internet Policy Review*, 31 marzo 2023.

MOBILIO G., *La Corte EDU condanna il ricorso alle tecnologie di riconoscimento*

facciale per reprimere il dissenso politico: osservazioni a partire dal caso Glukhin c. Russia, in *DPCE Online*, 62(1), 2024.
MOENSSENS A.A.-MEAGHER S.B., *Fingerprints and the law*, disponibile su http://www.crime-scene-investigator.net/fingerprintsourcebkchp13.pdf.
MOLINARI F.M., *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 3, 2013, p. 1259.
MONATERI P.G., *Diritti senza tempo né spazio*, in *Sole24ore*, 23 dicembre 2012.
MONTECCHI G.-VENUDA F., *Manuale di biblioteconomia*, Editrice Bibliografica, Milano, 1999.
MONTELEONE A., *Rilevazioni biometriche: lo stato della "privacy" delle "networked persons" tra il nuovo Codice ed i provvedimenti del Garante italiano*, in *Diritto&Diritti*, 2004.
MONTESANO L., *Le "prove atipiche" nelle presunzioni e negli "argomenti" del giudizio civile*, in *Riv. dir. proc.*, 1980, p. 246.
MOORE A.D. (a cura di), *Privacy, Security and Accountability. Ethics, Law and Policy*, Rowman & Littlefield, New York, 2016.
MORDINI E., *Il Volto e il Nome. Implicazioni Etiche, Sociali e Antropologiche delle Tecniche di Identificazione Biometriche*, in *MEDIC*, 14, 2006, p. 29-40.
MORDINI E.-OTTOLINI C., *Implicazioni etiche e sociali della biometria*, in *L'Arco di Giano*, 45, 2005, p. 67.
MORDINI E.-PETRINI C., *Ethical and social implications of biometric identification technology*, in *Ann Ist Super Sanità*, 43(1), 2007, p. 5-11.
MORELLI F., *Accertamenti e rilievi non ripetibili: una disciplina forse non incostituzionale, e tuttavia da rivisitare profondamente*, in *Giur. cost.*, 6, 2017, p. 2468.
MORRISON G.S., *Consensus on validation of forensic voice comparison*, in *Science & Justice*, Vol. 61, Issue 3, 2021, p. 299-309.
MURA A., *Teorema di Bayes e valutazione della prova*, in *Cass. pen.*, 2004, p. 1814.
MUSSO R.G., *Il processo penale statunitense. Soggetti ed atti*, Giappichelli, Torino, 2001.

NAGEL E., *La struttura della scienza*, IV ed., Feltrinelli, Milano, 1984.
NAIMOLI C., *Principio di falsificazione tra prova indiziaria e prova scientifica: riflessioni sul caso Garlasco e M. Kercher*, Pacini giuridica, Pisa, 2017.
NANAVATI S.-THIEME M.-NANAVATI R., *Biometrics. Identity verification in a networked world*, in *Wiley Computer Publishing*, 2002, p. 13-14.
NAPPI A., *Il prelievo ematico tra esigenza probatoria di accertamento del reato e garanzia costituzionale della libertà personale. Note a margine di un mancato bilanciamento tra valori*, in *Giur. cost.*, 1996, p. 2151.
NAPPI A., *Guida al codice di procedura penale*, IX ed., Giuffrè, Milano, 2004.

NAPPI A., *Libertà e legalità della prova in età moderna e contemporanea*, in *Cass. pen.*, 2012, p. 408 ss.

NARDOCCI C., *La (seconda) svolta del 2024. Anche il Consiglio d'Europa decide di regolamentare l'intelligenza artificiale*, in *BioLaw Journal-Rivista di BioDiritto*, Special Issue 1, 2024.

NEGRI D. (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Aracne, Roma, 2007.

NEGRI D., *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, 63(1), 2020.

NERONI REZENDE I., *Facial recognition in police hands: Assessing the "Claerview case" from a European perspective*, in *NJECL*, 11(3), 2020, p. 375 ss.

NERONI REZENDE I., *Facial Recognition for Preventive Purposes: The Human Rights Implications of Detecting Emotions in Public Spaces*, in L. BACHMAIER WINTER-S. RUGGERI (eds.), *Investigating and Preventing Crime in the Digital Era. Legal Studies in International, European and Comparative Criminal Law*, Vol. 7, Springer, Cham, 2022.

NERONI REZENDE I., *Glukhin and the EU regulation of facial recognition: Lessons to be learned?*, in *European Law Blog*, 19 settembre 2023.

NERONI REZENDE I., *Can we use AI and neuroscience to detect lies in criminal proceedings? A European perspective*, in www.limablog.org, 2024.

NEWTON D.E., *Dna Evidence and Forensic Science*, Infobase, New York, 2008.

NICOLICCHIA F., *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Dir. pen. cont.*, 2, 2018.

NICOLICCHIA F., *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Wolter Kluwer, Milano, 2020.

NIEVA-FENOLL J., *Intelligenza artificiale e processo*, trad. a cura di P. Comoglio, Giappichelli, Torino, 2019.

NOBILI M., *Concetto di prova e regime di utilizzazione degli atti nel nuovo codice di procedura penale*, in *Foro it.*, 1989, c. 274.

NOBILI M., *Il nuovo 'diritto delle prove' ed un rinnovato concetto di prova*, in *Leg. pen.*, 1989, p. 395 ss.

NOBILI M., *La nuova procedura penale. Lezioni agli studenti*, Clueb, Bologna, 1989.

NOBILI M., *Art. 188 c.p.p.*, in M. CHIAVARIO (a cura di), *Commento al nuovo codice di procedura penale*, vol. II, Utet, Torino, 1990, p. 396 s.

NOBILI M., *Il diritto delle prove ed un rinnovato concetto di prova*, in M. CHIAVARIO (a cura di), *Commento al nuovo codice di procedura penale*, vol. II, Utet, Torino, 1990.

NOBILI M., *sub art. 189* c.p.p., in M. CHIAVARIO (a cura di), *Commento al nuovo codice di procedura penale*, vol. II, Utet, Torino, 1990.
NOBILI M., *sub art. 191* c.p.p., in M. CHIAVARIO (a cura di), *Commento al nuovo codice di procedura penale*, vol. II, Utet, Torino, 1990.
NOBILI M., *sub art. 192* c.p.p., in M. CHIAVARIO (a cura di), *Commento al nuovo codice di procedura penale*, vol. II, Utet, Torino, 1990.
NOBILI M., *Scenari e trasformazioni del processo penale*, Cedam, Padova, 1998.
NOBILI M., *Storie d'una illustre formula: il "libero convincimento" negli ultimi trent'anni*, in *Riv. it. dir. proc. pen.*, 2003.
NOCERINO W., *Sulle modalità di acquisizione delle immagini provenienti dalle telecamere di videosorveglianza*, in *Cass. pen.*, 7-8, 2024, p. 2422.
NOFRI M., *Obbligatorio l'esame dibattimentale del perito già escusso in sede di incidente probatorio ex art. 392 comma 2 c.p.p.*, in *Giur. it.*, 1999, c. 383.
NUNIN R., *Utilizzo dei dati biometrici da parte del datore di lavoro: la prescrizione del Garante per la privacy*, in *Lav. giur.*, 2007, 2.
NUNZIATI M., *Note sul riconoscimento del parlante*, su http://www.teutas.it/societa-informazione/prova-elettronica/381-note-sul-riconoscimento-del-parlante.html.
NUVOLONE P., *Le prove vietate nel processo penale nei paesi di diritto latino*, in *Riv. dir. proc.*, 1966, p. 442 ss.

OATLEY G.-EWART B., *Data mining and crime analysis*, in *Wiley Interdisciplinary Reviews (WIREs): Data Minining and Knowledge Discovery*, 1(2), 2011, p. 147-153.
ORLANDI R., *Atti e informazioni dell'autorità amministrativa nel processo penale: contributo allo studio delle prove extracostituite*, Giuffrè, Milano, 1992.
ORLANDI R.-PAPPALARDO G., *L'indagine genetica nel processo penale germanico: osservazioni su una recente riforma*, in *Dir. pen. e proc.*, 1999, p. 762 ss.

PACE A., voce *Libertà personale (dir. cost.)*, in *Enc. dir.*, XXIV, Milano, 1974.
PAGALLO U., *Introduzione alla filosofia digitale. Da Leibniz a Chaitin*, Giappichelli, Torino, 2005.
PAGALLO U., *La tutela della privacy negli Stati Uniti d'America e in Europa. Modelli giuridici a confronto*, Giuffrè, Milano, 2008.
PAGALLO U., *Intelligenza Artificiale e diritto. Linee guida per un oculato intervento normativo*, in *Sist. intell.*, 3, 2017, p. 615 ss.
PAGALLO U., *Algo-Rhythms and the Beat of the Legal Drum*, in *Philos. Technol.*, 31, 2018, p. 507-524.
PAJNO A.-DONATI F.-PERRUCCI A. (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol. 1, *Diritti fondamentali, dati personali e regolazione*, il Mulino, Bologna, 2022.
PALERMO G.B.-MASTRONARDI V.-AGOSTINI S., *Il processo investigativo e*

accusatorio negli Stati Uniti d'America e in Italia, in *Suppl. Riv. di psich.*, 47(4), 2012, p. 42S-45S.

PALIOTTA A.P., *Le politiche innovative di sicurezza nelle città tra tecnologie di riconoscimento* e *smart cities*, in *SINAPPSI-Connessioni tra ricerca e politiche pubbliche*, 2, 2020.

PALMIOTTO F., *Le indagini informatiche e la tutela della riservatezza informatica*, in *Leg. pen.*, 1 luglio 2019.

PALMIOTTO F., *When is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis*, 2023, su https://ssrn.com/.

PALMIOTTO F., *Climbing a Wall: Strategic Litigation Against Automated Systems in Migration and Asylum*, in *German Law Journal*, Vol. 25, Special Issue 6: *Strategic Litigation in EU Law*, 2024, p. 935-955.

PALMIOTTO F., *Procedural fairness in automated asylum procedures: Fundamental rights for fundamental challenges*, in 50 *Computer Law & Security Review*, 55, 2024, 106065, p. 1-10.

PALMIOTTO F., *The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation*, in *EJRR*, 2025, p. 1-24.

PALMIOTTO F.-MENÉNDEZ GONZÁLEZ N., *Facial recognition technology, democracy and human rights*, in 50 *Computer Law & Security Review*, 3, 2023.

PANZAVOLTA M., *I profili dell'istituto*, in *Giur. it.*, 2010, p. 1222.

PANZAVOLTA M., *Legalità e proporzionalità nel diritto processuale penale*, in R. MASTROIANNI-O. POLLICINO-S. ALLEGREZZA-O. RAZZOLINI-F. PAPPALARDO, *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, Milano, 2017.

PAOLONI A., *La voce come elemento di identificazione della persona*, in A. DE DOMINICIS (a cura di), *La voce come bene culturale*, Carocci, Roma, 2002.

PAOLONI A., *Identificazione personale in ambito forense*, in *Mondo Digitale*, 2014, p. 6.

PAOLUCCI F., *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *Medialaws*, 1, 2021.

PARK U.-TONG Y.-JAIN A.K., *Age-invariant face recognition*, in *IEEE Trans. Pattern Anal. Mach. Intell.*, 32(5), p. 947954, May 2010.

PARKHI O.M.-VEDALDI A.-ZISSERMAN A., *Deep face recognition*, in *Proceedings of the British Machine Vision Conference (BMVC)*, 2015, p. 41.1-41.12.

PARLATO L., *Il riconoscimento facciale: vantaggi e insidie alla luce della giurisprudenza della corte EDU*, in P. DI SIMONE-A. MANGIARACINA-L. PARLATO, *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, Palermo University Press, Palermo, 2023.

PARODI C.-SELLAROLI V., *Sistema penale e intelligenza artificiale: molte esperienze e qualche equivoco*, in *Dir. pen. cont.*, 6, 2019.

PASCUCCI N., *La natura controversa della ricognizione fotografica*, in *Riv. it. dir. proc. pen.*, 1, 2017.
PASQUALE F., *The Black Box Society: The Secret Algorithms that Control Money and Information*, Cambridge, London, 2015.
PASQUINUCCI A., *Biometria e Sicurezza informatica*, in *ICT Security* n. 39-40-41-42, 2005-2006, si veda http://www.ucci.it/docs/ICTSecurity-2006-42.pdf.
PASSAIN M., *La privacy è morta, viva la privacy. Tutti i modi in cui veniamo controllati, spiati, schedati. Tutto quello che occorre sapere per difendersi*, Adriano Salani Editore, Firenze, 2009.
PATANÉ V., *Il diritto al silenzio dell'imputato*, Giappichelli, Torino, 2006.
PATO J.N.-MILLETT L.I. (eds.), *Biometric Recognition: Challenges and Opportunities*, in *The National Academies Press*, su http://www.nap.edu/catalog.php?record_id=12720.
PERFETTI T., *Biometria tra privacy e sicurezza*, su *www.computerlaw.it.*
PERONI F.-GIALUZ M. (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, EUT-Edizioni Università di Trieste, Trieste, 2009.
PERRI P., *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè, Milano, 2020.
PETERSON G.-SHENOI S., *Advances in Digital Forensics*, Springer, Orlando, 2009.
PEZZUTO R., *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, in *Dir. pen. cont.*, 1/2019.
PICARD R.W., *Affective Computing*, Cambridge, 2000.
PICCIRILLI G., *La "riserva di legge". Evoluzioni costituzionali, influenze sovrastatuali*, Giappichelli, Torino, 2019.
PICOTTI L. (a cura di), *Il diritto penale dell'informatica*, Cedam, Padova, 2004.
PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. e proc.*, 2008, 700.
PICOZZI M.-INTINI A., *Scienze forensi. Teoria e prassi dell'investigazione scientifica*, Utet, Torino, 2009.
PISAPIA G.D., voce *Errore giudiziario (riparazione dell')*, *II) Dir. proc. pen.*, in *Enc. giur.*, XIII, Roma, 1989, 2.
PITTIRUTI M., *Digital evidence e procedimento penale*, Giappichelli, Torino, 2017.
PIVATY A., *Suspects' privilege against self-incrimination not violated when made to unlock smartphone with fingerprint, Dutch Supreme Court rules*, in *Fair Trials*, 2021.
PIZZETTI F. (a cura di), *Intelligenza artificiale, protezione dati personali e regolazione*, Giappichelli, Torino, 2018.
PIZZI C., *Abduzione e serendipità nella scienza e nel diritto*, in *Cass. pen.*, 2005, p. 234 ss.

POISSON S.D., *Recherches sur la probabilitè des jugements en matière criminelle et en matière civile*, Imprimeur-libraire, Parigi, 1837.
POLIDORO D., *Tecnologie informatiche e procedimento penale: la giustizia penale messa alla prova dall'intelligenza artificiale*, in *Arch. pen.* (Web)3, 2020.
POLLICINO O.-PAOLUCCI F., *I limiti all'attività di polizia: dati biometrici e genetici solo con il controllo del giudice*, in *Il Sole 24 Ore*, 17 dicembre 2024.
POLLICINO O.-FROSINI T.E.-APA E. (a cura di), *Diritti e libertà in internet*, Mondadori, Milano, 2017.
PONZANELLI G., *Scienza, verità e diritto: il caso Bendectin*, in *Foro it.*, IV, 1994, c. 184.
POPPER K.R., *Scienza e filosofia*, Einaudi, Torino, 1969.
POPPER K.R., *Logica della scoperta scientifica*, Einaudi, Torino, 1970.
PORCU F., *Le videoriprese nel processo penale. Tra sicurezza, riservatezza e documentazione*, Wolters Kluwer Cedam, Milano, 2024.
POTETTI D., *Art. 228 comma 3 c.p.p.: il "perito istruttore"*, in *Cass. pen.*, 1997, p. 1544.
PREITE G., *Il riconoscimento Biometrico: Sicurezza vs. Privacy*, UNI Service, Trento, 2008.
PREITE G., *Politica e biometria. Nuove prospettive filosofiche delle scienze sociali*, Tangran edizioni scientifiche, Trento, 2016.
PRESUTTI A., *L'acquisizione forzosa dei dati genetici tra adempimenti internazionali e impegni costituzionali*, in *Riv. it. dir. e proc. pen.*, 53(2), 2010, p. 547-559.
PRETTI D., *Prime riflessioni a margine della nuova disciplina delle intercettazioni*, in *Dir. pen. cont.*, 1, 2018, p. 189 ss.
PRETTI D., *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni*, in *Sist. pen.*, 2020, p. 71 ss.
PRINS C., *Biometric Technology Law, Making Our Body Identify for us: Legal Implications of Biometric Technologies*, in 159 *CLSR*, 14(3), 1998.
PROCACCINO A., *Prove atipiche*, in A. GAITO (a cura di), *La prova penale*, I, Utet, Torino, 2009, p. 268.
PULICE M., *Sistemi di rilevazione di dati biometrici e privacy*, in *Lav. giur.*, 10, 2009, p. 994.
PULITANÒ D., *Il diritto penale fra vincoli di realtà e sapere scientifico*, in *Riv. it. dir. proc. pen.*, 2006, p. 802 ss.
PULITO L., *Il trattamento dei dati personali in ambito penale e l'uso del passenger name record per contrastare il terrorismo e altri reati gravi*, in *Proc. pen. e giust.*, 6, 2018, p. 1148.
PUTIGNANO D.S., *L'errore scientifico nel processo penale. Rilievi pratici e riscontri giurisprudenziali*, Giuffrè, Milano, 2007.

QUAGLIA A.-EPIFANO C.M. (a cura di), *Face recognition: methods, applications and technology*, NOVA Publishers, Enschede, 2010.

QUATTROCOLO S., *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali ed informatiche*, in *Leg. pen.*, 18 dicembre 2018.

QUATTROCOLO S., *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Rev. Italo-espanola derecho procesal*, 2019, 1.

QUATTROCOLO S., *Equo processo e sfide della società algoritmica*, in *BioLaw Journal-Riv. di BioDiritto*, 1, 2019, p. 135-144.

QUATTROCOLO S., *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, in *Cass. pen.*, 4, 2019, p. 1748-1765.

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

QUATTROCOLO S., *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws, Saggi – Focus: innovazione, diritto e tecnologia: temi per il presente e il futuro*, 2020.

QUATTROCOLO S., *Giustizia penale e intelligenza artificiale: finestre su uno scenario da esplorare*, in A. PAJNO-F. DONATI-A. PERRUCCI, *Intelligenza artificiale e diritto: una rivoluzione?*, vol. 2, il Mulino, Bologna, 2022, p. 533-540.

QUATTROCOLO S., *Il diritto delle prove penali alla luce della 'quarta rivoluzione'*, in C. CAMARDI (a cura di), *Collana del Centro Studi Giuridici del Dipartimento di Economia di Ca' Foscari, atti del Convegno "La via europea per l'intelligenza artificiale"*, Venezia il 25-26 novembre 2021, Wolters Kluwer Cedam, Milano, 2023.

QUATTROCOLO S., *L'ammissione della prova alla luce della rivoluzione digitale*, in E.M. CATALANO-P. FERRUA (a cura di), *Corderiana*, Giappichelli, Torino, 2023.

QUATTROCOLO S., *Prova e intelligenza artificiale*, in CONTI C.-MARANDOLA A. (a cura di), *La prova scientifica*, Giuffrè, Milano, 2023, p. 467-493.

QUATTROCOLO S., *Intelligenza artificiale e processo penale: le novità dell'AI ACT*, in *Dir. dif.*, 16 gennaio 2025.

QUATTROCOLO S.-SACCHETTO E., *EU&AI: Lessons to be learned*, in E. LIM-P. MORGAN (eds.), *Private Law and Artificial Intelligence*, Cambridge University Press, Cambridge, 2024, p. 636 ss.

QUATTROCOLO S.-ANGLANO C.-CANONICO M.-GUAZZONE M., *Techical Solutions for Legal Challenges: Equality of Arms in Criminal proceeding*, in *Global Jurist*, 20(1), 2020.

QUINTAVALLA A.-TEMPERMAN J. (eds.), *Artificial Intelligence and Human Rights*, Oxford University Press, Oxford, 2023.

RAFARACI T., *Ricognizione informale dell'imputato e (pretesa) fungibilità delle forme probatorie*, in *Cass. pen.*, 1998, p. 1741.

RAFFIOTTA E.C.-BARONI M., *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, in *BioLaw Journal-Riv. BioDiritto*, 2022, p. 165 ss.

RAMACHANDRA R.-STOKKENES M.-MOHAMMADI A.-VENKATESH S.-RAJA K.-WASNIK P.-POIRET E., MARCEL S.-BUSCH C., *Smartphone Multi-modal Biometric Authentication: Database and Evaluation*, in *Journal of latex class files*, 14(8), 2015.

RAMAIOLI S., *Rilievi dattiloscopici: aspetti medico-legali ed efficacia probatoria*, in *Mass. ann. Cass. pen.*, 1980, p. 1143.

RAMEN R.V.-YAMPOOLSKIY V., *Biometrics: a survey and classification*, in *Biometrics*, 11(1), 2008.

RANALDI G., *Processo penale e prova informatica: profili introduttivi*, in *Dir. pubbl. eur. Online*, 2, 2020.

RAPOSO V.L., *Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence*, in *Int. Journal of Law and Inform. Tech.*, Vol. 30, Issue 1, Spring 2022, p. 88-109.

RAPOSO V.L., *The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal*, in *Eur. J. Crim. Policy Res.*, 29, 2023, p. 515-533.

RAPOSO V.L., *When facial recognition does not 'recognise': erroneous identifications and resulting liabilities*, in *AI & Soc*, 2023.

RAPOSO V.L.-DU L., *Facial recognition technology: is it ready to be used in public health surveillance?* in *Int. Data Privacy Law*, Vol. 14, Issue 1, 2024, p. 66-86.

RATHA N.K.-CONNELL J.H.-BOLLE R.M., *Enhancing security and privacy in biometrics-based authentication systems*, in *IBM Systems Journal*, 40(3), 2001, p. 614-634.

RATTANI A.-DERAKHSHANI R., *A Survey Of mobile face biometrics*, in *Computers & Electrical Engineering*, 72, 2018, p. 39-52.

REITH M.-CARR C.N.-GUNSH G., *An Examination of Digital Forensic Models*, in *International Journal of Digital Evidence*, Vol. 1, Issue 3, 2002, p. 6-7.

RENZETTI S., *La prova scientifica nel processo penale: problemi e prospettive*, in *Riv. dir. proc.*, 2, 2015.

RESTA F.-POLLICINO O., *Riconoscimento facciale e protezione dati: attenzione al punto di non ritorno*, in *Diritti Comparati – Comparare i diritti fondamentali in Europa*, 30 gennaio 2020.

REUBEN M.-MORLEY J., *Investigation into the use of photoanthropometry in facial image comparison*, in *Forensic science int.*, 212(1), 2011, p. 231-237.

RICCI A., *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati. Riflessioni sul d.lgs. 18 maggio 2018, n. 51, di attuazione della dir. 2016/680/UE*, in *Nuove leggi civ. comm.*, 42(3), 2019, p. 565-598.

RICCI R., *La prova del DNA per la ricerca della verità: aspetti giuridici, biologici e probabilistici*, Giuffrè, Milano, 2006.
RICCI U., *DNA e crimine: dalla traccia biologica all'identificazione genetica*, Laurus Robuffo, Roma, 2001, p. 108 ss.
RICCI U., *L'accreditamento ISO 17025:2005 nel laboratorio di genetica forense*, in *Riv. it. med. leg.*, 1, 2014, p. 69.
RICCI U., *La qualità nel settore della genetica forense*, in *Riv. it. med. leg.*, 1, 2016, p. 233.
RICCI U., *Un lampo di consapevolezza nella normativa italiana: il DNA oltre la suggestione e il mito*, in *Dir. pen. e proc.*, 6, 2016, p. 751 ss.
RICCI U.-PREVIDERÈ C.-FATTORINI P.-CORRADI F., *La prova del Dna per la ricerca della verità. Aspetti giuridici, biologici e probabilistici*, Giuffrè, Milano, 2006.
RICCIO G., *Ragionando su intelligenza artificiale e processo penale*, in *Arch. pen.*, 3, 2019 (Web).
RICCIO G.M.-SCORZA G.-BELISARIO E. (a cura di), *GDPR e normativa privacy. Commentario*, I ed., Giuffrè, Milano, 2018.
RIVELLO P.P., voce *Perito e perizia*, in *Dig. disc. pen.*, IX, Torino, 1995, p. 478 ss.
RIVELLO P.P., *Il processo e la scienza*, in *Riv. it. dir. e proc. pen.*, 4, 2010, p. 1715.
RIVELLO P.P., *Tecniche scientifiche e processo penale*, in *Cass. pen.*, 4, 2013, p. 1691 ss.
RIZZO C., *Videoriprese in luoghi pubblici e poteri degli organi di polizia*, in *Cass. pen.*, 11/2024, p. 3584.
ROBERTS D.E., *Collateral Consequences, Genetic Surveillance, and the New Biopolitics of Race*, University of Pennsylvania Law School, Pennysylvania, 2011.
RODOTÀ S., *Tecnologie e diritti*, il Mulino, Bologna, 1995.
RODOTÀ S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 4, 1997, p. 606.
RODOTÀ S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997.
RODOTÀ S., *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012, p. 319.
RODOTÀ S., *Dal soggetto alla persona*, Editoriale scientifica, Napoli, 2007.
RODOTÀ S.-TALLACCHINI M. (a cura di), *Trattato di biodiritto*, vol. I, Giuffrè, Milano, 2011.
RODRIGUEZ A.M.-GERADTS Z.-WORRING M., *Likelihood Ratios for Deep Neural Networks in Face Comparison*, in *J. For. Sc.*, 2020, p. 5 ss.
ROMANO M., *Commentario sistematico del codice penale*, vol. I, Giuffrè, Milano, 2004.
ROSANÒ A., *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'unione europea: le proposte della commissione europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence)*, in *Leg. pen.*, 16 ottobre 2020.

ROSS A.-SHAH J.-JAIN A.K., *From Template to Image: Reconstructing Fingerprints From Minutiae Points*, in *IEEE Transactions on Pattern Analysis and Machine Intelligence, Special Issue on Biometrics*, 29(4), 2007, p. 544-560.

RUFFOLO U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020.

RUFFOLO U.-RICCIO G.-URICCHIO A.F., *Intelligenza Artificiale tra etica e diritti*, Cacucci, Bari, 2020.

RUGANI G., *La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della direttiva (UE) 2016/680: frammentazione ed incertezze applicative*, in *Freedom, Security & Justice: European Legal Studies Rivista quadrimestrale on line sullo Spazio europeo di libertà, sicurezza e giustizia*, 1, 2019.

RUGGERI S. (a cura di), *Human Rights in European Criminal Law. New Developments in European Legislation and Case Law after the Lisbon Treaty*, Springer, Cham, 2015.

RULLI E., *Giustizia predittiva, intelligenza artificiale e modelli probabilistici. Chi ha paura degli algoritmi?*, in *Il Mulino Rivisteweb, An. giur. econ.*, 2, 2018.

RUOTOLO M., voce *Habeas corpus* in M. FLORES (a cura di), *Diritti umani. Cultura dei diritti e dignità della persona nell'epoca della globalizzazione*, vol. II, Utet, Torino, 2007.

RUSSEL S.-PERSET K.-GROBELNIK M., *Updates to the OECD's definition of an AI system explained*, 29 novembre 2023, reperibile su https://oecd.ai/en/wonk/ai-system-definition-update.

SACCHETTO E., *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Dir. pen. cont.-Riv. trim.*, 2, 2019.

SACCHETTO E., *Biometrics as forensic evidence: some reflections from the Italian Criminal point of view*, in *IWBF*, 2020, p. 1-4.

SACCHETTO E., *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *Leg. pen.*, 16 ottobre 2020.

SACCHETTO E., *Brevi riflessioni sui fondamenti e sui limiti del rapporto fra* automated faced-based human recognition technology *e processo penale*, in A. PAJNO-F. DONATI-F. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione? Amministrazione, responsabilità, giurisdizione*, il Mulino, Bologna, 2022.

SACCHETTO E., *Automated faced-based human recognition technologies e procedimento penale alla luce della proposta di regolamento sull'IA: alcuni spunti di riflessione*, in C. CAMARDI (a cura di), *Collana del Centro Studi Giuridici del Dipartimento di Economia di Ca' Foscari, atti del Convegno "La via europea per l'intelligenza artificiale"*, Venezia il 25-26 novembre 2021, Wolters Kluwer Cedam, Milano, 2023.

SACCHETTO E., *La prova biometrica*, in C. CONTI-A. MARANDOLA, *La prova scientifica*, Giuffrè, Milano, 2023, p. 243-264.
SACKS M.J.-KOEHLER J.J., *The Individualization Fallacy in Forensic Science Evidence*, 2008, p. 219-220, disponibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1432516.
SALARDI S., *Dna ad uso forense: paladino di giustizia o reo di ingiustizie?*, in *Riv. it. med. leg.*, 6, 2011, p. 1359.
SALLANTIN J.-SZCZECINIARZ J.J., *Il concetto di prova alla luce dell'intelligenza artificiale*, Giuffrè, Milano, 2005.
SANGUINETI L., *La valutazione della prova*, Giuffrè, Milano, 1979.
SANTOSUOSSO A., *Diritto, scienza, nuove tecnologie*, Wolters Kluwer Cedam, Padova, 2016.
SANTOSUOSSO A., *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Mondadori, Milano, 2020.
SANTOSUOSSO A., *Diritto, scienza, nuove tecnologie*, III ed., Wolters Kluwer Cedam, Padova, 2021.
SAPONARO L., *Dall'indizio alla prova indiziaria: il rapporto tra probabilità e certezza*, Wolters Kluwer Cedam, Padova, 2015.
SAPONARO L., *L'impatto processuale delle immagini: fotografie e videoriprese*, Wolters Kluwer Cedam, Padova, 2020.
SAPONARO L., *Le nuove frontiere dell'individuazione personale*, in *Arch. pen.*, 1, 2022.
SARTOR G., *Intelligenza artificiale e diritto. Un'introduzione*, Giuffrè, Milano, 1996.
SARTOR G., *L'intelligenza artificiale e il diritto*, Giappichelli, Torino, 2022.
SARTOR G.-LAGIOIA F., *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, European Parliament, Brussels, 2020.
SARZANA C., *Evoluzione tecnologica e diritti dell'individuo*, in *Dir. inf.*, 1992, p. 393-411.
SARZANA C.-IPPOLITO S., *Informatica, internet e diritto penale*, Giuffrè, Milano, 2010.
SCAFFARDI L. (a cura di), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, Giappichelli, Torino, 2018.
SCAFFARDI L. (a cura di), *La Banca dati italiana del Dna. Limiti e prospettive della genetica forense*, il Mulino, Bologna, 2019.
SCAFFARDI L., *Forensic genetics: the evolving challenge of DNA cross-border exchange*, in *BioLaw Journal-Riv. di BioDiritto*, Special Issue 1, 2021, p. 329 ss.
SCAFFARDI L., *Next Generation Prüm e le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, in *Federalismi.it*, 8, 2021, p. 200 ss.

SCAGLIARINI S., *La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio*, Aracne, Roma, 2013.
SCALFATI A., *Gli accertamenti tecnici dell'accusa*, in *Ind. pen.*, 1992.
SCALFATI A., voce *Consulenza tecnica (dir. proc. pen.)*, in *Enc. giur.*, VIII, Roma, 1997.
SCALFATI A., *La deriva scientista dell'accertamento penale*, in *Proc. pen. giust.*, 5, 2011, p. 144.
SCALFATI A. (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2014.
SCALFATI A., *Note minime su cooperazione investigativa e mutuo riconoscimento*, in *Proc. pen. giust.*, 2017, p. 217 s.
SCALFATI A. (a cura di), *Pre-investigazioni (Espedienti e mezzi)*, Giappichelli, Torino, 2020.
SCALFATI S. (a cura di), *Novità su impugnazioni penali e regole di giudizio*, Ipsoa, Milano, 2006.
SCAPARONE M., *Evoluzione e involuzione del diritto di difesa*, Giuffrè, Milano, 1980.
SCAPARONE M., *sub art. 24 c. 2 Cost.*, in *Comm. Cost. Branca*, Zanichelli-Foro italiano, Bologna-Roma, 1981.
SCAPARONE M., *Elementi di procedura penale. I principi costituzionali*, Giuffrè, Milano, 1999.
SCAPARONE M., *Procedura penale*, vol. I, II ed., Giappichelli, Torino, 2010.
SCARCELLA A. (a cura di), *Prelievo del DNA e banca dati nazionale*, Cedam, Padova, 2009.
SCARSCELLA A., *Condizioni dell'efficacia probatoria nell'indagine dattiloscopica*, in *Dir. pen. e proc.*, 1, 2012, p. 68.
SCARCELLA A., *Conservazione delle impronte digitali degli "assolti" e violazione dell'art. 8 Conv. e.d.u.*, in *Dir. pen. e proc.*, 7, 2013, p. 809.
SCELLA A., *L'inutilizzabilità della prova nel sistema del processo penale*, in *Riv. it. dir. e proc. pen.*, 1992, p. 203 ss.
SCHAPEL H., *The New Approach to the New Approach: The Juridification of Harmonized Standards in EU Law*, in *Maastr. Journ. of Eur. and Comp. Law*, 20(4), 2013, p. 521-533.
SCHELLINO D., *Corte costituzionale e accertamenti peritali coattivi incidenti nella sfera corporale della persona*, in *Leg. pen.*, 1990, p. 173 ss.
SCHERER K.R.-WALLBOTT H.G., *Evidence for universality and cultural variation of differential emotion response patterning*, in *Journal of personality and social psychology*, 66(2), 1994, p. 310-28.
SCHRÖDER A., *"Real-time" versus "post" remote biometric identification systems under the AI Act*, in *ALTI Forum*, 14 ottobre 2022.
SCHWEITZER N.J.-SACKS M.J., *The CSI effect: popular fiction about forensic science affects the public's expectations about real forensic science*, in *Jurimetrics J.*, 47, 2007, p. 358.

SCIPIONE J.-LO MONACO M., *Has the horse bolted? Dealing with legal and practical challenges of facial recognition*, in *Media Laws*, 18 gennaio 2022.
SCOMPARIN L., *La tutela del testimone nel processo penale*, Cedam, Padova, 2000.
SEAMAN J.A., *Black Boxes*, in *Emory Law Journal*, 58(2), 2008, p. 427-488.
SECKINERA D.-MALLETTA X.B.-ROUXA B.C.-MEUWLY D.-MAYNARDA P., *Forensic image analysis – CCTV distortion and artefacts*, in *Foren. Science Intern.*, 285, 2018, p. 77-85.
SEMINARA S.-DE MAGLIE C. (a cura di), *Scienza e causalità*, Cedam, Padova, 2006.
SERRAO D'AQUINO P., *La responsabilità civile per l'uso di sistemi di intelligenza artificiale nella Risoluzione del Parlamento europeo 20 ottobre 2020: "Raccomandazioni alla Commissione sul regime di responsabilità civile e intelligenza artificiale"*, in *giustiziainsieme.it*, 18 novembre 2021.
SHALEV-SHWARTZ S.-BEN-DAVID S., *Understanding Machine Learning: From Theory to Algorithms*, Cambridge University Press, New York, 2014.
SICA S.-D'ANTONIO V.-RICCIO G.M. (a cura di), *La nuova disciplina europea della privacy*, Giuffrè, Milano, 2016.
SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa.* Giappichelli, Torino, 2018.
SIMONCINI A., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal-Rivista di BioDiritto*, 1, 2019, p. 63-88.
SINGH M.-NAGPAL S.-SINGH R.-VATSA M., *On Recognizing face images with weight and age variations*, in *Proc. IEEE Digital Object Identifier*, 2, 2014.
SIRACUSANO D., *Studio sulla prova delle esimenti*, Giuffrè, Milano, 1959.
SIRACUSANO D., *Introduzione allo studio del processo penale*, Giuffrè, Milano, 1989.
SIRACUSANO D., voce *Prova*, in *Enc. giur.*, XXV, Roma, 1991.
SIRACUSANO F., *Tra semplificazione e ibridismo: insidie e aporie dell'Ordine europeo di indagine penale*, in *Arch. pen.*, 2017, n. 2.
SLOBOGIN A., *Public privacy: camera surveillance of public spaces*, 2002, p. 219-223, consultabile su http://www.olemiss.edu/depts/ncjrl/pdf/LJournal02Slobog.pdf.
SMUHA N. *et al.*, *How the Eu can achieve legally trustworthy AI: a response to the European Commission's Proposal for an Artificial Intelligence Act*, su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991.
SMUHA N.A.-AHMED-RENGERS E.-HARKENS A.-LI W.-MACLAREN J.-PISELLI R.-YEUNG K., *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, 2021, su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991.
SMYTH S., *Biometrics, surveillance and the law. Societies of restricted access, discipline and control*, Routledge, New York, 2019.

SORELL M., *Video provenance by motion vector analysis: A feasibility study*, in *International Symposium on Communications, Control, and Signal Processing* (*ISCCSP*), 2012.
SPAGNOLO P., *Il Tribunale della libertà. Tra normativa nazionale e normativa internazionale*, Giuffrè, Milano, 2008.
SPAGNOLO P., *La nuova cooperazione giudiziaria penale: mutuo riconoscimento e tutela dei diritti fondamentali*, in *Cass. pen.*, 3, 1 marzo 2020, p. 1290.
SPANGHER G., *«E pur si muove» dal male captum bene retentum alle esclusionary rules*, in *Giur. cost.*, 2001, p. 2829 ss.
SPANGHER G. (diretto da), *Trattato di procedura penale*, Utet giuridica, Torino, 2011.
SPINELLA A.-SOLLA G., *L'identificazione personale nell'investigazione scientifica: DNA e impronte*, in *Cass. pen.*, 1, 2009, p. 428 ss.
SPINNEY L., *The Fine Print*, in *Nature*, vol. 464, 18 marzo 2010.
STEFANI E. (a cura di), *Il processo penale accusatorio*, Giuffrè, Milano, 2013.
STEFANINI E., *Dati genetici e diritti fondamentali*, Cedam, Padova, 2008.
STELLA F., *Leggi scientifiche e spiegazione causale del diritto penale*, Giuffrè, Milano, 2000.
STELLA F., *Giustizia e modernità. La protezione dell'innocente e la tutela delle vittime*, III ed., Giuffrè, Milano, 2003.
STELLA F. (a cura di), *I saperi del giudice. La causalità e il ragionevole dubbio*, Giuffrè, Milano, 2004.
STONE M., *La cross-examination. Strategie e tecniche*, Giuffrè, Milano, 1990.
STONEY D.A., *Measurement of Fingerprint Individuality*, in *Advances in Fingerprint Technology*, 327, 329, 2001.
STUMPF J.P., *The Crimmigration Crisis: Immigrants, Crime, and Sovereign Power*, in *Amer. Univ. Law Review*, 56(2), 2016, p. 367 ss.
SUBRAMANIAN B.-KIM J.-MARAY M.-PAUL A., *Digital Twin Model: A Real-Time Emotion Recognition System for Personalized Healthcare*, in *IEEE Access*, 10, 2022, p. 81155-81165.

TADDEI ELMI G.-CONTALDO A. (a cura di), *Intelligenza artificiale. Algoritmi giuridici Ius condendum o "fantadiritto"?*, Pacini, Pisa, 2020.
TAEIHAGH A., *Governance of artificial intelligence*, in *Policy and Society*, 2021.
TAGLIARO F.-D'ALONA E.-SMITH F.P., *L'ammissibilità della prova scientifica in giudizio e il superamento del Frye standard: note sugli orientamenti negli Usa successivi al caso Daubert v. Merrel Down Pharmaceuticals, Inc.*, in *Riv. it. med. leg.*, 2000, p. 719.
TAIGMAN Y.-YANG M.-RANZATO M.-WOLF L., *DeepFace: closing the gap to human-level performance in face verification*, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2014, p. 1701-1708.

TALLACCHINI M., *Bodyright. Corpo biotecnologico e diritto*, in *Biblioteca della libertà*, 1998, p. 21-50.
TALLACCHINI M., *Il corpo e le sue parti. L'allocazione giuridica dei materiali biologici umani*, in *Med. e Mor.*, 1998, p. 499-544.
TALLACCHINI M., *Retorica dell'anonimia e proprietà dei materiali biologici umani*, in F. D'AGOSTINO (a cura di), *Corpo esibito, corpo violato, corpo venduto, corpo donato. Nuove forme di rilevanza giuridica del corpo umano*, Giuffrè, Milano, 2003, p. 171-192.
TARUFFO M., *Certezza e probabilità nelle presunzioni*, in *Foro it.*, 1974, c. 83.
TARUFFO M., *Il diritto alla prova nel processo civile*, in *Riv. dir. proc.*, 1984, p. 77.
TARUFFO M., *Modelli di prova e di procedimento probatorio*, in *Riv. dir. proc.*, 1990, p. 420.
TARUFFO M., *La prova dei fatti giuridici. Nozioni generali*, Giuffrè, Milano, 1992.
TARUFFO M., *Judicial decision and Artificial Intelligence*, in *Art. Intel. and Law*, 1998, p. 311 ss.
TASPINAR M.-NASKALI A.T.-EREN G.-KURT M., *The importance of customized advertisement delivery using 3D tracking and facial recognition*, in *2012 Second International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, 2012, p. 520-524.
TAULLI T., *Artificial Intelligence Basics*, Apress, Berkeley, 2019.
TERESI C., *L'AI Act nell'ottica del processual-penalista: uno sguardo preliminare*, in *Riv. pen. dir. e proc.*, 20 giugno 2024.
TERRACIANO U., *La metodologia dell'investigazione*, Franco Angeli, Milano, 2014.
TESSITORE G., *Riconoscimento automatico del volto e confronto in ambito forense*, in P. DI SIMONE-A. MANGIARACINA-L. PARLATO, *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, Palermo University Press, Palermo, 2023.
TESTAGUZZA A., *Digital Forensics. Informatica giuridica e processo penale*, Wolters Kluwer Cedam, Milano, 2014.
THOMPSON W.C.-TARONI F.-AITKEN C.G.G., *How the probability of a False Positive Affects the Value of Dna Evidence*, in *J. Forensic Science*, 48(1), Jan. 2003, p. 1-2.
TIANI V., *Olimpiadi 2024, come funziona la sicurezza tech*, 23 luglio 2024, in www.wired.it.
TISTARELLI M.-CHAMPOD C. (eds.), *Handbook of Biometrics for Forensic*, Springer, Cham, 2017.
TOMKINS S.S., *Affect, imagery, consciousness*, Vol. 1, *The positive affects*, Springer, New York, 1962.

TONINI P., *Il valore probatorio dei documenti contenenti dichiarazioni scritte*, in *Cass. pen.*, 1990, p. 2212.
TONINI P., *Problemi insoluti della prova documentale*, in *Dir. pen. e proc.*, 1996.
TONINI P., *Il contraddittorio: diritto individuale e metodo di accertamento*, in *Dir. pen. e proc.*, 2000, p. 1388.
TONINI P., *La prova penale*, Cedam, Padova, 2000.
TONINI P. (a cura di), *Giusto processo. Nuove norme sulla formazione e valutazione della prova*, Cedam, Padova, 2001.
TONINI P., *Prova scientifica e contraddittorio*, in *Dir. pen. e proc.*, 2003, p. 1459 ss.
TONINI P., *La prova scientifica nel processo penale*, suppl. a *Dir. pen. e proc.*, 6, 2008, p. 52.
TONINI P., *La prova scientifica: considerazioni introduttive*, in *Dir. pen. e proc.*, 6, 2008, *Dossier La prova scientifica nel processo penale*.
TONINI P., *Accertamento del fatto e informazioni genetiche: un difficile bilanciamento*, in *Dir. pen. e proc.*, 2009, *Dossier: Banca dati nazionale del DNA e prelievo di materiale biologico,* p. 3.
TONINI P., *Documento informatico e giusto processo*, in *Dir. pen. e proc.*, 2009, p. 403.
TONINI P., *La Cassazione accoglie i criteri Daubert sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza*, in *Dir. pen. e proc.*, 11, 2011, p. 1341 ss.
TONINI P., *Manuale di procedura penale*, Giuffrè, Milano, 2019.
TONINI P., *L'evoluzione delle categorie tradizionali: il documento informatico*, in A. MANNA-A. CADOPPI-S. CANESTRARI-M. PAPA (a cura di), *Cybercrime*, Utet, Torino, 2023, p. 1506.
TONINI P.-CONTI C., *Il diritto delle prove penali*, Giuffrè, Milano, 2012.
TORRE M., *Privacy e indagini penali*, Giuffrè, Milano, 2020.
TORRE M., *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. e proc.*, 8, 2021.
TOSI O., *Voice identification. Teory and Legal applications*, University Park Press, Baltimora, 1979.
TRAVERSI A., *Intelligenza artificiale applicata alla giustizia: ci sarà un giudice robot?*, in www.questionegiustizia.it.
TRAVERSO F., *Il diritto alla controprova nei rapporti con la perizia*, in *Dir. pen. e proc.*, 1998, p. 596.
TRIGGIANI N., *Le videoriprese investigative e l'uso dei droni*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2019, p. 61.
TRIGGIANI N., *Le videoriprese investigative tra Corte costituzionale e sezioni unite cronaca di una travagliata evoluzione giurisprudenziale (... in attesa del legislatore)*, in *Iurisdictio*, 4, 2023, p. 40-63.
TRINGALLI G., *Banche dati di Polizia: sussiste il diritto alla privacy e all'oblio?*, 24 settembre 2014, disponibile su http://www.altalex.com/documents/

news/2014/10/10/banche-dati-di-polizia-sussiste-il-diritto-alla-privacy-e-all-oblio.
TROISI P., *L'errore giudiziario tra garanzie costituzionali e sistema processuale*, Cedam, Padova, 2011.
TSAMADOS A.-AGGARWAL N.-COWLS J. *et al.*, *The ethics of algorithms: key problems and solutions*, in *AI & Soc.*, 37, 2022, p. 215-230.
TURING A., *Intelligenza meccanica*, Bollati Boringhieri, Torino, 1994.

UBERTIS G., *Fatto e valore nel sistema probatorio penale*, Giuffrè, Milano, 1979.
UBERTIS G. (a cura di), *La conoscenza del fatto nel processo penale*, Giuffrè, Milano, 1992.
UBERTIS G., *La prova penale. Profili giuridici ed epistemologici*, Giappichelli, Torino, 1995.
UBERTIS G., *Sistema di procedura penale*, Giappichelli, Torino, 2004.
UBERTIS G., voce *Giusto processo (diritto processuale penale)*, in *Enc. dir.*, *Annali*, II, t. 1, Milano, 2008.
UBERTIS G., *La tutela del contraddittorio e del diritto di difesa tra CEDU e Trattato di Lisbona*, in *Cass. pen.*, 2010, p. 2494.
UBERTIS G., *Il giudice, la scienza, la prova*, in *Cass. pen.*, 2011, p. 4112 ss.
UBERTIS G., *Profili di epistemologia giudiziaria*, Giuffrè, Milano, 2015.
UBERTIS G., *Considerazioni generali su investigazioni e prove transnazionali*, in *Cass. pen.*, 1, 2017, 50.

VACIAGO G., *Digital Evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli, Torino, 2012.
VALLI R., *Le indagini scientifiche nel procedimento penale*, Giuffrè, Milano, 2013.
VAN BUSKIRK E.-LIU V.T., *Digital Evidence: Challenging the Presumption of reliability*, in *Journal of Digital Forensic Practice*, 2006 (1), 20.
VAN DER PLOG I., *Biometric identification technologies: ethical implications of the information of the body. Biometric Technology & Ethics*, in *BITE Policy* Paper, no. 1, 2005.
VAN DIJK P.-VAN HOOF G.H.J., T*heory and Practice of the European Convention on Human Rights*, III ed., Martinus Nijoff, Leiden, 1998, p. 430 ss.
VAN NATTA M. *et al.*, *The rise and regulation of thermal facial recognition technology during the Covid-19 pandemic*, in *Journal of Law and the Biosciences*, 7(1), 2020.
VASSALLI G., *Il diritto alla libertà morale (Contributo alla teoria dei diritti della personalità)*, in *Studi in memoria di Filippo Vassalli*, II, Utet, Torino, 1960, p. 1629 ss.
VASSALLI G., *Il diritto alla prova nel processo penale*, in *Riv. it. dir. proc. pen.*, 1968, p. 2 ss.

VAVOULA N., *Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism*, in *European Journal of Migration and Law*, 23(4), 2021, p. 457-484.
VECCHIO F., *Le intercettazioni da remoto e i diversi modelli di bilanciamento tra esigenze investigative e diritto alla riservatezza e all'integrità dei sistemi informatici*, in *La Cittadinanza europea*, 1, 2016, p. 107-127.
VECELLIO SEGATE R., *Biometric Technology at the Borders of Citizenship: Identifying Technical Standards for Introducer-Based Remote Onboarding in Global Contexts of Statelessness, Nomadism, Displacement, and Refuge*, in *International Journal of Digital Law and Governance*, 1(2), 2024, p. 313-360.
VERSTA L.G., *Voiceprint identification*, Nature, New York, 1962.
VESSIO G., *Intelligenza artificiale per curiosi. Una mini-guida scientifica per tutti*, Edizioni Dedalo, Bari, 2025.
VICOLI D., *Riflessioni sulla prova scientifica: regole inferenziali, rapporti con il sapere comune, criteri di affidabilità*, in *Riv. it. med. leg.*, 2013, p. 1239 ss.
VIGONI D., *Corte costituzionale, prelievo ematico coattivo e test del Dna*, in *Riv. it. dir. e proc. pen.*, 4, 1996, p. 1022.
VIOLA P.-JONES M., *Rapid Object Detection Using a Boosted Cascade of Simple Features*, in *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2001, p. 511 ss.
VOENA G.P., voce *Difesa: III) difesa penale*, in *Enc. giur.*, Roma, 1989.

WACHTER S., *Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond*, in *Yale Journal of Law and Technology*, 26(3), 2024, p. 671, 716.
WACHTER S.-MITTELSTADT B.-FLORIDI L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017.
WALTL B.-VOGL R., *Explainable Artificial Intelligence – the New Frontier in Legal Informatics*, in *Jusletter* IT, 22 febbraio 2018.
WANG W., *Il manuale del giovane hacker*, Tecniche nuove, Milano, 2006.
WARREN S.D.-BRANDEIS L.D., *The right of privacy*, in 4 *Harvard Law Review* 193, 1890.
WATCHER S.-MITTLESTADT B.-FLORIDI L., *Why a right to explanation of automated decision-making does not exist in the GDPR*, in *Int. Data Privacy Law*, 7, 2017, p. 76 ss.
WAYMAN J.L., a *Definition of "Biometrics"*, in *National Biometric Test Center Collected Works*, 2000.
WAYMAN J.L., *The History of Information Security: A Comprehensive Handbook*, Elsevier, Amsterdam, 2007.
WAYMAN J.-JAIN A.-MALTONI D.-MAIO D., *Biometric Systems. Technology, Design and Perfomance Evaluation*, Springer, London, 2005.

WAYMAN J.-MCIVER R.-WAGGETT P.-CLARKE S.-MIZOGUCHI M.-BUSCH C.-DELVAUX N.-ZUDENKOV A., *Vocabulary harmonisation for biometrics: the development of ISO/IEC 2382 Part 37*, in *The Institution of Engineering and Technology*, Vol. 3, Issue 1, March 2014, p. 1-8.
WAYMAN J.L., *Fundamentals of biometric authentication technology*, in *Proceedings cardtech/securtech*, Chicago, 1999.
WAYMAN J.L., *Fundamentals of biometric authentication technologies*, in *Int. J. Image Graphics*, 1(1), 2001, p. 93-113.
WEST E.M., *Court Findings of Prosecutorial Misconduct Claims in Post-Conviction Appeals and Civil Suits Among the First 255 Dna Exoneration Cases*, 2010, disponibile su https://www.nacdl.org/WorkArea/DownloadAsset.aspx?id.
WOODS T.P., *The Implicit Bias of the Implicit Bias Theory*, in *Drexel Law Review*, 2017, p. 631 ss.
WOODWARD J.D.-ORLANS N.M.-HIGGINGS P.T., *Identity Biometrics*, McGraw-Hill, 2003.
WOODWARD J.D.-HORN C.-GATUNE J.-THOMAS A., *Biometrics A Look at Facial Recognition in Public Safety and Justice*, RAND, Santa Monica, 2003.

ZACCHÉ F., *La prova documentale*, Giuffrè, Milano, 2012.
ZALNIERIUTE M., *Burning Bridges: the automated facial recognition technology and public space surveillance in the modern State*, in *Colum. Sci. & Tech. L. Rev.*, 22, 2021, p. 284 ss.
ZALNIERIUTE M., *Glukhin v. Russia. App. No. 11519/20. Judgment*, in *Amer. Journal of Int. Law*, 117(4), 2023, p. 699.
ZAPPALÀ E., *Il principio di tassatività dei mezzi di prova nel processo penale*, Giuffrè, Milano, 1982.
ZATIKO K., *Commentary: Defining digital forensics*, in *Forensic Magazine*, 2007, disponibile su http://www.forensicmag.com/node/128.
ZAVRSNIK A., *Criminal justice, artificial intelligence systems and human rights*, in *ERA* Forum, 2020.
ZENO-ZENCOVICH V., voce *Identità personale*, in *Dig. disc. priv., sez. civ.*, IX, Torino, 1993, p. 294-303.
ZICCARDI G., *Scienze forensi e tecnologie informatiche: la computer and network forensics*, in *Inf. e dir.*, XV(2), 2006, p. 103-125.
ZICCARDI G., *L'avvocato hacker. Informatica giuridica e uso consapevole (e responsabile) delle tecnologie*, Giuffrè, Milano, 2012.
ZICCARDI G., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina, Milano, 2015.
ZIOSI M.-HEWITT B.-JUNEJA P.-TADDEO M.-FLORIDI L., *Smart Cities: Mapping their Ethical Implications*, 5 gennaio 2022, reperibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4001761.

ZIROLDI A., *Intelligenza artificiale e processo penale tra norme, prassi e prospettive*, in *Quest. giust.*, 18 ottobre 2019.

ZONTEK W., *Biometric Encryption of Smart Devices and the Prohibition against Self-incrimination in Criminal Procedure. Old Guarantees in the New World*, in *EJCCLCJ*, 32, 2024, p. 156-174.

ZUBOFF S., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Roma, 2019.

ZUCCONI V., *Pena di morte, la svolta dell'FBI*, in *La Repubblica*, 12 gennaio 2006.

Finito di stampare nel mese di giugno 2025
nella Stampatre s.r.l. di Torino
Via Bologna, 220

Memorie del Dipartimento di Giurisprudenza
dell'Università degli Studi di Torino

Volumi pubblicati

1. Ruggero Rudoni, *Il principio di legalità delle sanzioni 'penali' in una prospettiva costituzionale nazionale ed europea*, 2024.
2. Isabella Alberti, *L'istruttoria nel procedimento amministrativo. Prospettive di acquisizione digitale della conoscenza*, 2024.
3. Chiara Castaldo, *Libertà individuali e* open data. *Gli obblighi di servizio pubblico nella gestione dei dati*, 2024.
4. Fabrizio Sudiero, *La segnalazione dell'organo di controllo* ex *art. 25-*octies *del Codice della crisi d'impresa e dell'insolvenza*, 2025.
5. Sergio Foà (a cura di), *Il nuovo merito amministrativo*, 2025.
6. Maura Mattalia, *Contenzioso climatico e condizioni dell'azione avanti al giudice amministrativo*, 2025.
7. Ernestina Sacchetto, *Tecnologie di riconoscimento facciale e procedimento penale. Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna*, 2025.