UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di diritto pubblico, internazionale e comunitario

CORSO DI LAUREA IN DIRITTO E TECNOLOGIA

a.a. 2022/2023

Tesi di laurea

L'impiego delle tecnologie di riconoscimento facciale per la prevenzione e la repressione dei reati

Relatore:

Prof.re Massimo Bolognari

Studente:

Michela Caprin

[Mat.: 2010482]

INDICE

Introduzione

La rivoluzione digitale ha condotto inevitabilmente alla digitalizzazione della biometria, consentendo a quest'ultima di diventare parte integrante della quotidianità della nostra società. Si consideri l'implementazione di sistemi di riconoscimento delle impronte digitali su dispositivi mobili personali, l'introduzione della firma grafometrica nel contesto della documentazione bancaria, sino a giungere alla possibilità di autenticazione, offerta dai nostri cellulari, grazie al riconoscimento del volto. Tali tecnologie hanno notevolmente semplificato l'accesso alla tecnologia.

Parimenti, gli strumenti di riconoscimento biometrico hanno ottenuto rapidamente notevole successo anche nell'ambito delle attività investigative condotte dagli organi di polizia. Il recente avvento dell'intelligenza artificiale apre nuove prospettive per lo sfruttamento delle tecnologie di riconoscimento facciale a scopi di prevenzione e repressione del crimine. Tuttavia, come si avrà modo di analizzare nel corso della trattazione, l'identificazione automatica dei cittadini è un sistema che si presenta attualmente ancora nella sua fase embrionale, comportando sfide di non poco momento e gravide di implicazioni.

Da un lato vi è il rischio che un utilizzo illegittimo dei *software* di riconoscimento facciale possa condurre ad una lesione dei diritti degli interessati. Dall'altro lato, ci si interroga sull'effettiva funzionalità di questa tecnologia.

Alla luce delle suesposte osservazioni, il presente elaborato si prefigge di analizzare il complesso rapporto tra biometria e processo penale, esaminando, in particolare, la possibilità di utilizzo del dato biometrico facciale come prova all'interno del processo. Il lavoro si concentra poi, in ottica comparata tra Italia e Regno Unito, sull'analisi del processo di riconoscimento, verificandone il funzionamento, le opportunità offerte e l'impatto sui diritti fondamentali riconosciuti a livello internazionale.

Capitolo I

Biometria e processo penale: due mondi che si intrecciano

1.1. La biometria

La biometria rappresenta la "disciplina che studia le grandezze biofisiche allo scopo di identificarne i meccanismi di funzionamento, di misurarne il valore e di indurre un comportamento desiderato in specifici sistemi tecnologici"[1]. Tale disciplina è da molto tempo riconosciuta come uno degli strumenti più efficaci di cui si servono le autorità, in ambito processuale penale, al fine di prevenire e reprimere il crimine, poiché consente di individuare soggetti di cui è ignota l'identità. In concreto una tale operazione è possibile grazie al processo di autenticazione biometrica, attraverso il quale si procede ad un'attenta osservazione di talune caratteristiche anatomiche, fisiologiche e comportamentali[2] proprie di ciascun soggetto e che permettono di distinguere un individuo rispetto ad un altro. Il dato che si ottiene attraverso la biometria è peculiare e distintivo, in quanto non può essere rilevato "sulla base di una semplice raccolta dati"[3], ma è l'*output* "di uno specifico processo tecnico"[4] che esplora le caratteristiche del soggetto in esame[5].

Il termine biometria è genericamente utilizzato per riferirsi sia al dato biometrico grezzo che è possibile ottenere a seguito dello studio delle caratteristiche tipiche di ciascun soggetto, ma anche con riferimento agli specifici strumenti tecnologici di identificazione e autenticazione che permettono la verifica dell'identità degli individui[6]. Il processo biometrico ha un duplice scopo: "la verifica della dichiarazione d'identità di un soggetto"[7] e "l'attribuzione di un'identità ad un soggetto ignoto"[8].

---

[1] Definizione di "biometria" da Enciclopedia Treccani Online. https://www.treccani.it/enciclopedia/biometria consultato il 12/06/2023

[2] E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Diritto Penale e Uomo*, Milano, fascicolo 5/2021, (p. 70)

[3] L. GRECO, A. MANTELERO, *Industria 4.0, robotica e privacy-by-design*, in *Diritto dell'Informazione e dell'Informatica (II)*, fasc. 6 01/12/2018, (p. 883)

[4] L. GRECO, A. MANTELERO, *Industria 4.0, robotica e privacy-by-design*, in *Diritto dell'Informazione e dell'Informatica (II)*, fasc. 6 01/12/2018, (p. 884)

[5] *Ibidem*

[6] E. SACCHETTO, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Diritto penale contemporaneo*, fascicolo 2/2019, (p. 467)

[7] CNIPA, *Linee guida per le tecnologie biometriche* versione del 08/10/2004, (p. 11)

[8] *Ibidem*

La biometria rappresenta pertanto lo strumento idoneo a definire il grado di coincidenza delle caratteristiche biometriche rilevabili in un individuo e confrontate con quelle di altri soggetti, svolgendo una comparazione del tipo "uno a molti", nel processo di identificazione.

Le regole per le elaborazioni e l'interpretazione dei risultati, la definizione dei parametri e la codifica degli stessi sono tutti caratteri predeterminati dalla biometria[9].

1.1.1. Dato biometrico

I dati ottenibili grazie alla biometria sono molteplici e di natura eterogenea: taluni sono il risultato dell'osservazione di caratteristiche comportamentali di un individuo, ad esempio, il riconoscimento vocale e le peculiarità grafometriche. Altri invece appartengono allo studio di caratteristiche anatomiche e fisiologiche del soggetto potendone così ottenere le impronte digitali, la geometria della mano ed i tratti del volto[10]. Nonostante l'eterogeneità della loro natura i dati biometrici presentano delle caratteristiche essenziali comuni.

Il dato biometrico è, anzitutto, universale. Tutti gli individui possiedono, nella generalità dei casi, gli "stessi elementi fisici"[11]: due occhi, una bocca, due mani, specifiche impronte digitali. Naturalmente gli elementi indicati subiscono delle variazioni in relazione alle peculiarità che caratterizzano ciascun individuo[12]. Si parla al riguardo di distinguibilità del dato biometrico. Infatti, benché gli elementi fisici siano propri di tutti gli esseri umani, questi presentano caratteristiche biometriche uniche per taluna persona.

Ulteriore profilo caratterizzante del dato biometrico è rappresentato dalla sua natura permanente. Infatti, la tipicità di ciascun dato biometrico è destinata a rimanere tale in

---

[9] N. BALOSSINO, S. Siracusa, *L'identificazione basata sul volto: metodi fisionomici e metrici*, in *Security Forum*, 2004.

[10] E. SACCHETTO, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Diritto penale contemporaneo*, fascicolo 2/2019, (p. 467) ed E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Diritto Penale e Uomo*, Milano, fascicolo 5/2021, (p. 70)

[11] *Ibidem*

[12] CNB, *L'identificazione del corpo umano: profili bioetici della biometria*, 26 novembre 2010, (p. 6)

modo quasi inalterato per l'intera vita di una persona[13]. Infine, ciascun dato biometrico ricavabile è soggetto a collezionabilità, potendo essere raccolto, utilizzato e riutilizzato[14]. Per poter procedere al confronto di queste tipologie peculiari di dati è necessario il previo consenso dell'interessato.

Inoltre, la procedura non deve comportare un onere eccessivo e l'utilizzo di metodologie a carattere invasivo non tollerate dall'individuo, motivo per cui il rilevamento dei dati e la loro successiva misurazione dovrebbero consistere in una procedura semplice, rapida e segnatamente rispettosa della dignità dell'individuo e delle sue garanzie[15].

Il dato biometrico rappresenta, dunque, una "forma di digitalizzazione del corpo umano"[16] il quale si trasforma in una fonte essenziale di informazioni, che risultano essere di estrema utilità in ambito investigativo. Gli elementi anatomici presenti nel nostro corpo rappresentano una sorta di "codice a barre"[17], analogo a quello che è possibile osservare sui prodotti commerciali per consentirne univocamente l'identificazione. La nostra pelle, i tratti del nostro volto, le caratteristiche dei nostri occhi sono, infatti, gli elementi che ci permettono di distinguerci dagli altri.

1.1.2. Il dato biometrico alla luce del GDPR e della Direttiva UE 680/2016 e il diritto all'identità personale

Fornire una definizione di dato biometrico rappresenta un'operazione solo all'apparenza semplice, ma che in realtà appare particolarmente problematica. Le tecnologie attualmente in grado di rilevare tali dati evolvono velocemente e la quantità e qualità di informazioni ottenibili aumenta esponenzialmente, coinvolgendo sempre maggiori tratti fisici umani.

---

[13] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 137)
[14] *Ibidem*
[15] *Ibidem*
[16] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 136) Cfr I. VAN DER PLOEG, *Biometric identification technologies: ethical implications of the informatization of the body*. Biometric Technology & Ethics, BITE Policy Paper no.1, 2005.
[17] *Ibidem*

Il Regolamento UE 679/2016 e la Direttiva UE 680/2016 tentano di darne una definizione quanto più ampia possibile, definendo il dato biometrico come "dato personale ottenuto da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quale l'immagine facciale o i dati dattiloscopici"[18]. In base a questa definizione, dunque, il dato biometrico costituisce una categoria particolare di dati personali. Essi ricevono una tutela rafforzata nell'articolo 9 Regolamento Generale sulla Protezione dei dati che ne vieta il trattamento al di fuori delle deroghe previste dallo stesso.
Trattandosi di una categoria speciale di dati personali il Garante europeo per la Protezione dei dati stabilisce che il loro trattamento deve essere subordinato al perseguimento di un interesse pubblico rilevante. In caso contrario si avrebbe un trattamento illecito[19]. Tuttavia, il perseguimento di un interesse pubblico non rappresenta una ragione sufficiente per il trattamento in esame, ma deve essere anche considerata la proporzionalità del processo e l'adozione di specifiche misure di sicurezza in grado di salvaguardare i diritti fondamentali propri di ciascun interessato[20].

Il dato biometrico è soggetto alla stringente disciplina della Direttiva UE 2016/680, che ha carattere speciale rispetto a quella fissata dal Regolamento 2016/679/UE, qualora sia utilizzato per finalità di repressione e prevenzione del crimine. L'art. 10 Direttiva stabilisce che il trattamento di dati biometrici è autorizzato solo se risulta essere strettamente necessario, sottoposto a garanzie adeguate e in presenza delle seguenti condizioni: sia stato autorizzato dal diritto dell'Unione o dello Stato Membro, sia idoneo a salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica, oppure riguardi dati resi espressamente pubblici dall'interessato[21].
Il trattamento di dati personali così descritto risulta essere un elemento potenzialmente lesivo dei diritti fondamentali, soprattutto quando venga in gioco in ambito investigativo. Fra le garanzie maggiormente esposte a rischio di venire violate spicca il diritto all'identità e all'immagine personale, dato che il dato biometrico rivela elementi che

[18] Definizione fornita dall'art. 4 comma 14 GDPR
[19] Art. 9 comma 2 lettera g) GDPR
[20] E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Diritto Penale e Uomo*, Milano, fascicolo 5/2021, (p. 73)
[21] Art. 10 Direttiva UE 2016/680

permettono di individuare in maniera univoca un soggetto[22]. Il diritto all'identità personale ha rilievo costituzionale[23] nella misura in cui si riferisce sia al "pieno sviluppo della persona"[24], sia "all'interesse della comunità a conoscere la reale identità dei suoi componenti"[25].

Sempre con maggior frequenza le forze di polizia sfruttano il potenziale delle nuove tecnologie che consentono di ricavare i dati biometrici degli individui a partire dalle videoriprese di sorveglianza o dalle immagini segnaletiche dei sospettati. In questo modo, risulta più semplice risalire all'identità del soggetto ritratto. Tale tipologia di operazione si scontra evidentemente con l'interesse proprio di ciascuna persona "a non vedere travisato o alterato all'esterno il proprio patrimonio intellettuale, politico, sociale [e] religioso"[26] conseguentemente "all'attribuzione di idee, opinioni, o comportamenti"[27] diversi rispetto a quelli realmente manifestati dall'interessato[28]. La necessità di preservare e tutelare a tutti i costi la nostra identità trova il suo fondamento nella sua stessa funzione: l'identità è ciò che permette all'essere umano di essere distinto dagli altri suoi simili.
Se è pacifico che la necessità di identificare ciascun cittadino sia un elemento fondamentale all'interno di una società sviluppata, con particolare riferimento alle crescenti esigenze di sicurezza nei rapporti interpersonali, altrettanto pacifico è il contributo fornito dalla biometria in questa direzione[29]. Tuttavia, l'utilizzo di nuove metodologie tecnologicamente avanzate aumenta notevolmente il rischio di tramutare le operazioni di identificazione in occasioni di vero e proprio controllo sociale[30].
Di fronte a questa evoluzione l'interessato può sentirsi minacciato, poiché l'associazione degli elementi di rilevazione operata dalla macchina consente all'operatore di attribuire

---

[22] E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Diritto Penale e Uomo*, Milano, fascicolo 5/2021, (p. 79)
[23] Art. 2 Cost., Art. 3 Cost., Art. 13 Cost.
[24] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 62) Cfr P. BARILE, *Diritti dell'uomo e libertà fondamentali*, 1984, (p. 26)
[25] *Ibidem*
[26] G. PINO, *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali*, in *Libera circolazione e protezione dei dati personali*, 2006
[27] *Ibidem*
[28] *Ibidem*
[29] CNB, *L'identificazione del corpo umano: profili bioetici della biometria*, 26 novembre 2010, (p. 4)
[30] *Ibidem*

all'immagine di un volto il nome e cognome di una persona fisica, alla quale poi potranno essere associate per esempio carte di credito, passaporto, *password*, idee politiche e riferimenti alla propria condizione di salute[31]. Il rischio è ancor più evidente se si pensa che la metodologia utilizzata permette la portabilità dei dati raccolti in forma di stringa matematica e conservabili nei *server* in maniera permanente[32]. È così che il diritto all'identità personale viene facilmente messo in discussione, portando l'individuo a mutare i propri comportamenti in tutte le occasioni in cui egli percepisca che questo corre il rischio di subire un'ingiusta compressione di questa garanzia[33]. In dottrina tale comportamento modificativo delle proprie abitudini e autolimitativo nell'esercizio dei propri diritti fondamentali, quali la libertà di associazione e di espressione, prende il nome di *chilling effect* o effetto inibitore[34].

Il trattamento automatizzato dei dati biometrici può avvenire ad opera di diversi soggetti, talora anche ignoti all'interessato, e in modo occulto, ossia senza che l'interessato ne sia a conoscenza. Si tratta, dunque, di operazioni di cui l'individuo non ha il controllo ed idonee ad incidere significativamente la sua sfera più intima e privata.
Il diritto all'identità personale viene messo ulteriormente in pericolo nell'ipotesi in cui si verifichi una frammentazione dell'identità di un soggetto rispetto alla integralità della persona umana[35]. Talvolta, infatti, il trattamento dei dati può riguardare soltanto taluni dati che rappresentano solo una parte dell'identità e dell'individualità complessiva, giungendo in questo modo ad una rappresentazione parziale e fuorviante della persona[36]. La potenza delle tecnologie di riconoscimento facciale di decifrare le caratteristiche uniche dei volti e sintetizzarle in dati, svilendone il "valore simbolico, culturale e sociale di rappresentazione della personalità"[37] culmina nella riduzione delle persone a punteggi

---

[31] *Ibidem*
[32] CNB, *L'identificazione del corpo umano: profili bioetici della biometria*, 26 novembre 2010, (p. 5)
[33] *Ibidem*
[34] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale,* in *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, 2022, (p. 23)
[35] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 66)
[36] *Ibidem*
[37] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 67)

o profili, favorendo così i processi di decontestualizzazione lesivi del diritto fondamentale della persona all'identità personale[38].

Questo panorama porta dunque alla concretizzazione del timore, espresso in seno al Comitato Nazionale per la Bioetica, di una progressiva erosione del diritto all'identità personale come conseguenza delle crescenti esigenze di identificazione nelle società odierne[39].

1.1.3. Quando una foto non è più "solo una foto"

Fra le tecniche biometriche ad oggi disponibili, rileva in questo contesto la tecnologia di riconoscimento facciale, la quale si basa su una serie di procedimenti algoritmici, il cui *output* è l'identificazione di una persona a partire dall'immagine del suo volto[40]. Tale trattamento sfrutta immagini e video che riprendono il viso di un soggetto per risalire alla sua identità, confrontando in maniera automatizzata l'immagine estrapolata con un'altra dello stesso previamente identificato e contenuta in un *database*[41].

Fra le tecnologie biometriche, quelle in grado di riconoscere il volto di una persona possono ritenersi uniche. Difficilmente, infatti, potremmo riuscire a nascondere il nostro volto in maniera pacifica, mancando nella società occidentale un giustificato motivo religioso o culturale per apparire in luogo pubblico a volto completamento coperto. Pertanto, l'apprensione dell'immagine facciale appare più agevole rispetto, ad esempio, all'ottenimento di campioni biologici di DNA[42].

Tuttavia, non tutte le immagini sono idonee ad essere utilizzate per il riconoscimento facciale. L'algoritmo utilizzato sfrutta taluni punti di repere, ossia aree cutanee ridotte "corrispondenti a formazioni anatomiche facilmente riconoscibili"[43][44], per elaborare una

---

[38] *Ibidem*

[39] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 68)

[40] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 11)

[41] *Ibidem*

[42] *Ibidem*

[43] Come, ad esempio**,** la radice del naso, la punta più sporgente dello stesso, il punto più sporgente dell'ala del naso, la sporgenza del mento ed il punto più sporgente dello zigomo

[44] Definizione di "repere" in dizionario Treccani online. https://www.treccani.it/vocabolario/ricerca/repere/ consultato il 20/06/2023

sorta di cartografia del volto umano[45]. Risulta dunque particolarmente importante la qualità del fotogramma sottoposto ad esame, che influisce in modo decisivo sulla procedura di riconoscimento[46]. È necessario inoltre prendere in considerazione molteplici fattori di interferenza come la luminosità, deformazioni delle immagini introdotte dai dispositivi di acquisizione e, ancora, trasfigurazioni o occultamenti del volto che rendono difficoltoso il riconoscimento degli specifici aspetti facciali[47].

Ne consegue che, al fine di ottenere una corrispondenza accurata tra le immagini di volta in volta confrontate sarà necessario l'utilizzo di fotogrammi il più possibile nitidi, che ritraggano la persona preferibilmente priva di espressioni che alterino la conformazione del viso: smorfie o sorrisi potrebbero, infatti, pregiudicare il processo di identificazione[48]. Inoltre, dovrebbero essere preferite immagini ricavate in ambienti controllati. Si allude ai c.d. "sistemi biometrici interattivi"[49] ("laddove prevedono la cooperazione dell'interessato e richiedono la sua consapevole partecipazione durante la fase di raccolta del dato biometrico"[50]), che si riferiscono alle immagini segnaletiche apprese negli uffici di polizia, nelle quali è dedicata particolare attenzione all'inquadratura del soggetto e all'illuminazione circostante.

La natura del fotogramma estratto in un ambiente diverso, attraverso l'utilizzo di "sistemi biometrici passivi"[51], come, ad esempio, l'uso di una videocamera di sorveglianza all'interno di un locale pubblico, non è, invece, sempre idoneo a fornire immagini di cui l'operatore può usufruire, verificandosi talvolta casi in cui il soggetto viene ripreso da una distanza troppo elevata, di lato, il più delle volte in movimento e spesso non viene messo sufficientemente a fuoco dalla camera.

---

[45] N. BALOSSINO, S. SIRACUSA, *L'identificazione basata sul volto: metodi fisionomici e metrici*, in *Security Forum*, 2004.
[46] E. SACCHETTO, *Face to Face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *La legislazione penale*, 2020, (p. 3)
[47] N. BALOSSINO, S. SIRACUSA, *L'identificazione basata sul volto: metodi fisionomici e metrici*, in *Security Forum*, 2004.
[48] *Ibidem*
[49] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 32)
[50] Garante per la protezione dei dati personali, *Linee-guida in materia di riconoscimento biometrico e firma grafometrica. Allegato A al Provvedimento del Garante del 12 novembre 2014*, Gazzetta ufficiale della repubblica italiana, Serie generale n. 280, 02/12/2014, (p. 88)
[51] *Ibidem*

Cionondimeno, viene a doversi considerare anche la dubbia totale affidabilità dei risultati frutto dei processi di identificazione[52]. Seppur infatti tali sistemi offrano notevoli capacità di fornire risultati migliori rispetto a quanto sarebbe possibile elaborando i dati manualmente, questo non esclude la presenza costante di un certo margine di errore, anche se esso è da intendersi maggiore nei sistemi di riconoscimento del volto, rispetto a sistemi di riconoscimento delle impronte digitali[53]. Le condizioni che incidono in tale processo sono molteplici: si può fare riferimento a variazioni ambientali e fisiche, ma anche a livello di acquisizione e registrazione dei dati, ed ancora l'inattendibilità potrebbe derivare dal lasso di tempo troppo elevato intercorso tra il momento di acquisizione e quello di elaborazione e verifica dei dati raccolti[54]. Inoltre, particolare considerazione deve essere rivolta alla qualità dei risultati ottenibili attraverso tecniche automatizzate, si tratterebbe infatti di *output* con valenza meramente statistica e percentuale, implicando così un'inferenza pressoché incerta e contraria ai principi dell'accertamento penale[55].

In conclusione, sono evidenti le potenzialità proprie di una fotografia che ritrae il volto di una persona, poiché essa ne consente l'identificazione[56]. Ovviamente occorre sempre verificare la sua natura e la sua qualità, affinché essa possa essere utilizzata per svolgere un confronto accurato con altra immagine rappresentativa. Ai nostri giorni, scattarci una fotografia non appare più un'operazione del tutto innocua, ma significa "lasciare una traccia elettronica"[57], perlopiù indelebile, di noi stessi "nell'infosfera"[58].

---

[52] C. FANUELE, *Dati genetici e procedimento penale*. 2009, (p. 1, 2)
[53] E. SACCHETTO, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Diritto penale contemporaneo*, fascicolo 2/2019, (p. 475)
[54] *Ibidem*
[55] *Ibidem*
[56] Con i rischi che derivano sul piano dei diritti fondamentali, sui quali ci si soffermerà più avanti
[57] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, in *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, 2022, (p. 16)
[58] Terminologia di L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano 2017

1.2. La biometria come strumento funzionale al processo penale

L'esigenza di ottenere i dati biometrici di "imputati, arrestati o ricercati"[59] non è figlia del nuovo secolo, ma affonda le sue radici fin nel Seicento, epoca in cui già si avvertiva l'esigenza di raccogliere tutte le informazioni circa i tratti somatici del sospettato in modo quanto più minuzioso possibile, al fine di poterlo identificare in un momento successivo più agevolmente[60].

L'elaborazione di un preciso metodo scientifico di segnalamento descrittivo a scopo identificativo risale però alla fine del XIX secolo, grazie al lavoro dell'antropologo francese Alphonse Bertillon[61]. Tale metodologia prevedeva la misurazione, effettuata con specifici compassi, di undici parti del corpo umano, le quali erano funzionali alla classificazione in gruppi omogenei dei soggetti segnalati[62].

Le nuove tecnologie attualmente disponibili hanno reso più agevole il raggiungimento di questo obiettivo da parte delle forze dell'ordine, le quali possono contare su una maggior rapidità nell'esecuzione del confronto. Tra le opportunità offerte dalle nuove strumentazioni può pacificamente considerarsi l'elisione della "degradazione mnestica"[63] che tipicamente subisce la mente umana. La stessa impedirebbe all'essere umano di compiere ripetutamente il riconoscimento di un sospettato in modo minuzioso e veritiero (in ragione del progressivo sfumare dei ricordi), dovendosi così assumere che il riconoscimento compiuto da una persona fisica riferirebbe ad un'attività psicologicamente irripetibile[64]. Contrariamente a quanto vale per l'essere umano, il pregio della macchina risulta essere quello di memorizzare le immagini, analizzarle e riprodurle potenzialmente un numero infinito di volte[65]. Un esempio che dimostra le potenzialità dei sistemi di riconoscimento biometrico per la repressione dei reati è il caso in cui le forze dell'ordine ne usufruiscano per identificare i soggetti presenti sulla scena

---

[59] L. GARLATI, *Alle origini della prova scientifica: la scuola di polizia di Salvatore Ottolenghi*, in *Revista Brasileira de Direito Processual Penal*, volume 7 2021, (p. 885)
[60] E. MASINI, *Sacro arsenale ovvero Prattica dell'officio della Santa Inquisizione, Seconda Parte, Del modo di formare i processi, e esaminare Testimoni, e Rei*, in *Le vere radici dell'Europa*, 2022, (p. 51)
[61] N. BALOSSINO, S. SIRACUSA, *L'identificazione basata sul volto: metodi fisionomici e metrici*, in *Security Forum*, 2004.
[62] *Ibidem*
[63] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, in *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, 2022, (p. 15)
[64] *Ibidem*
[65] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, in *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, 2022, (p. 16)

del crimine. Un fotogramma tratto dalle immagini raccolte da una videocamera di sorveglianza, risulta essere molto più attendibile di una testimonianza oculare, che può essere influenzata da fattori ambientali e dalle inevitabili distorsioni rappresentative che caratterizzano la mente umana.

1.2.1. L'impiego del dato biometrico nel processo penale

Il dato biometrico frutto dell'elaborazione automatica operata dalla macchina può essere qualificato come prova digitale nell'ambito del processo penale[66], in quanto si tratta di un'informazione con valore probatorio memorizzata o trasmessa in formato digitale[67]. Richiedendo per la sua raccolta specifiche abilità tecnico-scientifiche, il dato biometrico può essere considerato una *species* del *genus* più ampio di prova scientifica, non godendo però di una regolamentazione specifica parimenti a quanto accade per quest'ultima[68].

La problematica maggiore dell'impiego del dato biometrico, soprattutto quello facciale, nel processo penale è dunque sicuramente tale lacuna normativa, a cui è correlato il rischio di un'assenza di garanzie adeguate a tutela degli interessati.
A questo proposito, a complicare ulteriormente il quadro, è intervenuto il D.lgs. 51/2018, che ha recepito la direttiva 2016/680/UE relativa alla protezione dei dati personali e che all'art. 7 prevede una riserva di legge in materia di trattamento dei dati[69]. Esso, infatti, è autorizzato "solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento, ovvero, ferme le garanzie dei diritti e delle libertà, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato. È dunque evidente che in tutti quei casi in cui non vi sia una specifica

---

[66] E. SACCHETTO, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Diritto penale contemporaneo*, fascicolo 2/2019, (p. 475)
[67] Definizione fornita dallo Scientific Working Group on Digital Evidence in https://www.swgde.org/glossary consultato il 01/07/2023
[68] E. SACCHETTO, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Diritto penale contemporaneo*, fascicolo 2/2019, (p. 475)
[69] L. SAPONARO, *Le nuove frontiere dell'individuazione personale*, in *Archivio penale – Rivista web*, fascicolo n. 1, 2022, (p. 10)

disposizione di legge, come accade per il caso delle immagini raccolte con tecniche di riconoscimento facciale, il trattamento dei dati debba essere ritenuto illegittimo.

Va poi verificata la compatibilità di tali strumenti con i principi costituzionali ove l'identificazione biometrica richieda il prelievo di materiale biologico grezzo dalla persona sottoposta all'indagine o incida significativamente nel diritto alla riservatezza proprio di ciascun soggetto[70].
Dottrina e giurisprudenza si interrogano ormai da tempo sulla possibilità di far coincidere la prospettiva garantistica propria del nostro ordinamento con l'esponenziale utilizzo da parte dell'Autorità di strumentazioni potenzialmente idonee a ledere i diritti fondamentali.

1.2.2. Biometria facciale e possibilità di utilizzo del dato biometrico come mezzo di prova atipico

Occorre domandarsi se il dato biometrico facciale possa essere ricondotto in via interpretativa all'interno dei mezzi di prova tipici, o se, invece, vada inquadrato nella categoria dei mezzi di prova atipici.

Sotto un primo profilo, si è cercato di ricondurre le tecnologie di riconoscimento facciale all'istituto della ricognizione fotografica di persone. In particolare, l'art. 213 c.p.p. prevede che, quando occorra procedere a ricognizione, il giudice invita colui che è chiamato ad eseguirla a descrivere la persona di interesse, indicandone tutti i particolari di cui ha memoria[71]. È evidente già in prima battuta la difficoltà riscontrabile nell'estendere tale disciplina alle tecnologie in esame. Il riconoscimento, infatti, in questo caso non verrebbe operato da un agente umano, bensì dalla macchina, la quale porterebbe a termine l'operazione in modalità automatizzata. Manca poi un riferimento esplicito ad un eventuale trattamento di dati biometrici.

[70] *Ibidem*
[71] Dispositivo dell'art. 213 c.p.p.

Altri hanno sostenuto che le tecnologie di riconoscimento facciale possano essere ricondotte all'identificazione (art. 349 c.p.p.). In base a tale norma la polizia giudiziaria procede "all'identificazione della persona nei cui confronti vengono svolte le indagini"[72], anche attraverso l'esecuzione di rilievi fotografici e antropometrici nel rispetto della libertà personale dell'interessato. Generalmente tali accertamenti, implicando una momentanea immobilizzazione per la descrizione, fotografia o misurazione di parti esposte del corpo umano, non pregiudicano la dignità o il diritto alla libertà personale. Tuttavia, il legislatore contempla la possibilità di un intervento coattivo a fini identificativi, previa autorizzazione da parte del P.M., per i casi in cui si renda necessario il prelievo di materiale biologico sull'indagato[73]. La sottoposizione del soggetto alla tecnologia di riconoscimento facciale non implica di per sé un intervento coattivo. Non parrebbe, dunque, giustificabile l'estensione delle garanzie previste in materia di identificazione per il caso in cui si renda necessario procedere coattivamente[74].

Occorre però considerare il caso in cui l'interessato non fornisca il proprio consenso a sottoporsi alla procedura di riconoscimento.

In questa circostanza il suo dissenso varrebbe quale espressione del proprio diritto a non collaborare nei termini di diritto a non fornire prove su sé stesso (art. 24 Cost.). Più in particolare, quando è la persona stessa a costituire l'oggetto della ricerca (e dunque è il suo corpo ad essere fonte di prova) il diritto a non fornire prove su sé stessi si esplica nella facoltà di rimanere immobili e non compiere alcun movimento fisico. Tuttavia, questo non esclude la possibilità per le forze dell'ordine di procedere comunque all'identificazione, soprattutto in considerazione del fatto che la mera ripresa dell'immagine facciale non dovrebbe comportare una compressione della libertà personale[75].

Ciononostante, quanto fintanto detto pare scontrarsi con il diritto alla libertà morale della persona nell'assunzione della prova, tutelato dall'art. 188 c.p.p.. Il dettato normativo vieta (a prescindere dall'ottenimento del consenso da parte dell'interessato) l'utilizzo di metodi

---

[72] Dispositivo dell'art. 349 c.p.p.
[73] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 87, 88)
[74] *Ibidem*
[75] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 89)

o tecniche che influiscano sulla libertà di autodeterminazione o alterino la capacità di ricordare e di valutare i fatti[76].

In particolare, "questa accezione di libertà morale può essere ricondotta al divieto di ogni violenza fisica e morale sulle persone"[77] sottoposte a restrizioni di libertà. L'utilizzo delle tecniche di riconoscimento facciale però non implica alcun rapporto diretto (che sembrerebbe invece richiesto) tra l'interessato e le forze di polizia, perciò il diritto alla libertà morale, inteso in questi termini, non parrebbe subire una lesione[78].

Se si assume però una concezione più ampia di libertà morale, le conclusioni saranno diverse. Infatti, il diritto *de quo* può essere inteso anche come una "forma di autodeterminazione nelle proprie scelte difensive e negli atteggiamenti processuali"[79]. In questi termini, la circostanza in cui l'autorità procede ad accompagnare coattivamente la persona presso gli uffici di polizia per procedere all'identificazione, determina inevitabilmente la violazione della libertà di autodeterminazione.

In aggiunta, la sottoposizione a riconoscimento facciale, in mancanza del consenso dell'interessato, o in maniera occulta, appare essere in contrasto con la garanzia del *nemo tenetur se detergere*[80]. In ambito biometrico, infatti, il corpo della persona è identificato come fonte di prova di natura dichiarativa; pertanto, rappresenta esso stesso un elemento in grado di ledere gli interessi del soggetto[81].

Un ulteriore tentativo operato dalla dottrina è stato quello di assoggettare il dato biometrico facciale alla disciplina che viene comunemente utilizzata per l'ingresso delle immagini all'interno del processo, ossia la normativa inerente alla prova documentale[82].

In assenza di un diretto riferimento normativo alle tecnologie di riconoscimento facciale, gli indirizzi elaborati sulle videoriprese forniscono degli spunti importanti. In particolare,

---

[76] Dispositivo dell'art. 188 c.p.p.

[77] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 90)

[78] *Ibidem*

[79] *Ibidem*

[80] Da intendersi quale caposaldo secondo cui nessuno può essere obbligato a fare dichiarazioni contrarie al proprio interesse.

[81] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 90, 91)

[82] L. SAPONARO, *Le nuove frontiere dell'individuazione personale*, in *Archivio penale – Rivista web*, fascicolo n. 1, 2022, (p. 15)

le riprese video e le prove che ne scaturiscono non sono di fatto una materia specificatamente regolata dalla legge. Tuttavia, il loro innegabile valore a livello processuale è stato pacificamente riconosciuto anche dalla giurisprudenza, la quale per legittimare il loro utilizzo e identificare la disciplina ad esse applicabile ha usufruito delle disposizioni riguardanti altre prove e principi processuali.

Un apporto significativo in questa direzione è stato fornito dalle Sezioni Unite che hanno distinto le videoriprese operate in luogo pubblico da quelle che avvengono in ambiente privato e, ancora, tra apprensioni in grado di captare contenuti comunicativi da quelle che invece non lo sono.

Con riferimento al caso di videoriprese pubbliche prive di contenuto comunicativo gli orientamenti giurisprudenziali espressi sono stati molteplici.
Fra questi, una parte della giurisprudenza ritiene che le videoriprese debbano essere assoggettate alle norme in materia di prova documentale. La ragione risiede nel contenuto stesso dell'art. 234 c.p.p., il quale ammette l'acquisizione di "documenti che rappresentano fatti, persone o cose mediante la fotografia […] o qualsiasi altro mezzo"[83].
Le tecnologie oggetto di trattazione sembrerebbero, dunque, idonee a rientrare in questa fattispecie, in quanto strumentazioni dalle quali è possibile ricavare soltanto immagini prive di audio.
Tuttavia, è da considerare che già di per sé il legittimo ingresso di immagini all'interno del procedimento penale appare essere il risultato di una manipolazione normativa operata a livello giurisprudenziale, pertanto un'ulteriore estensione alle videoriprese effettuate in ambito di riconoscimento facciale sarebbe da ritenere un azzardo che non ci si può permettere avendo coscienza dell'invasività propria di quest'ultime[84].

In conclusione, alla luce delle criticità in questa sede esaminate e delle peculiarità che caratterizzano la materia oggetto di trattazione, non può che ritenersi insoddisfacente il tentativo interpretativo di ricondurre le tecnologie di riconoscimento facciale nell'alveo delle prove tipiche.

---

[83] Dispositivo dell'art. 24 c.p.p.
[84] L. SAPONARO, *Le nuove frontiere dell'individuazione personale*, in *Archivio penale – Rivista web*, fascicolo n. 1, 2022, (p. 16, 17)

Viene quindi a doversi valutare la possibilità di applicare la disciplina delle prove atipiche.

In particolare, queste ultime rappresentano una categoria non disciplinata dalla legge, ma che il giudice può ammettere se "idonea all'accertamento dei fatti e non pregiudica la libertà morale della persona"[85]. È necessario però considerare il primo requisito richiesto dal legislatore per poter assumere una prova di questo tipo. Le tecnologie *de quo* sembrano attualmente inidonee ad assicurare l'accertamento dei fatti, mancando in molteplici casi[86] informazioni circa il loro funzionamento, nonché sulla percentuale di errore riscontrata nel sistema[87]. Allo stesso modo, anche la libertà morale della persona risulta subire una compressione di fronte all'utilizzo coatto, o occulto, di tali strumentazioni, dovendo necessariamente constatarsi una limitazione alla libertà di autodeterminazione del soggetto.

Per concludere, l'unica via percorribile per poter ammettere pacificamente in ambito processuale penale l'uso degli applicativi *de quo* sembra consistere nella previsione di una disciplina *ad hoc* da parte del legislatore, il quale, conformandosi alle indicazioni fornite della Corte di Giustizia europea[88], dovrebbe restringere l'applicazione di tali tecnologie alle fattispecie di reato più gravi, richiedendo un atto autorizzativo da parte del giudice o di un'autorità amministrativa indipendente[89].

[85] Dispositivo dell'art. 189 c.p.p.
[86] Ad esempio, si veda in proseguo il caso SARI
[87] E. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario* in *La legislazione penale*, 2021, (p. 214)
[88] Tra le molte pronunce assimilabili: CGUE, GS, 5 aprile 2022, C-140/20, G.D., §§ 59 e 106
[89] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, in *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, 2022, (p. 27)

Capitolo II

L'avvento dei sistemi di riconoscimento facciale in Italia

2.1. Il funzionamento del nuovo "occhio sociale"

La tecnologia di riconoscimento facciale è definibile quale "trattamento automatico di immagini digitali che contengono i volti di persone ai fini di identificazione, autenticazione/verifica o categorizzazione di tali persone"[90]. Il trattamento avviene sulla base di un procedimento preordinato al raggiungimento di specifiche finalità[91].

Tradizionalmente il processo biometrico finalizzato alla verificazione, talvolta detta anche autenticazione, consiste nel confronto tra due immagini del volto di una persona, al fine di stabilire se si tratta del medesimo soggetto[92]. Questa tipologia di trattamento si basa sul "confronto uno-a-uno"[93] e non richiede la memorizzazione delle caratteristiche facciali degli individui all'interno di un database centralizzato, ma è sufficiente la loro riproduzione all'interno di un documento, come, ad esempio, quello d'identità[94].

La tecnologia di riconoscimento facciale assolve anche scopi di categorizzazione degli individui in tutte le circostanze in cui essa viene sfruttata per catalogare le caratteristiche comuni di innumerevoli soggetti, quali il sesso, l'età e l'origine etnica potendosene così desumere i gruppi all'interno dei quali gli individui che presentano le stesse caratteristiche possono essere ricondotti[95]. Non si tratta di un processo che conduce direttamente all'identificazione di una persona, ma è possibile ottenere questo risultato se si procede

---

[90] Definizione fornita da Article 29 Data protection working party, in *Opinion 02/2012 on facial recognition in online and mobile services*, adottata il 22 Marzo 2012
[91] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 32)
[92] FRA – European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, (p. 7)
[93] *Ibidem*
[94] *Ibidem*
[95] FRA – European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, (p. 7)

all'associazione dei dati ottenuti con altre ulteriori informazioni che la riguardano, generando così l'*identikit* di ciascun individuo[96].

Ai nostri fini interessa, in particolare, il trattamento che caratterizza l'attività di riconoscimento operata dalle autorità di *law enforcement*, che consiste nell'identificazione.

La procedura può essere svolta in due modi. In modalità statica, operando un confronto tra l'immagine del volto dell'interessato con una moltitudine di altre fotografie contenute all'interno del *database* di riferimento, al fine di verificare se lo stesso soggetto è stato preventivamente registrato e conseguentemente se ne conoscono già le generalità[97]. Diversamente, quando opera in modalità *live* l'algoritmo analizza in diretta i flussi video ottenuti dalle videocamere di sorveglianza, estrapola "l'impronta facciale" dei soggetti ripresi e confronta l'immagine appresa con quelle contenute in un elenco stilato dagli operatori[98].

La differenza sostanziale tra le due riguarda il momento di elaborazione dei dati e dunque di identificazione.

Considerando la mole di dati analizzata, si può ritenere che venga effettuata una "comparazione uno-a-molti"[99].

L'*output* fornito dall'algoritmo di riconoscimento all'operatore è un risultato che indica la probabilità che le due immagini analizzate ritraggano la stessa persona[100]. In particolare, è possibile procedere all'identificazione prendendo in considerazione due *set* di dati differenti. In primo luogo, si può attingere a banche dati in cui a priori è già certa la possibilità di ottenere un punteggio di compatibilità elevato (c.d. "identificazione a *set*

---

[96] *Ibidem*
[97] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale,* in *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*. 2022, (p. 12)
[98] *Ibidem*
[99] FRA – European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, (p. 7)
[100] FRA – European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, (p. 9)

chiuso"[101]). In alternativa, si potrebbe procedere con una "identificazione a *set* aperto"[102], considerando un *database* in cui non è nota la presenza dell'interessato.

2.1.1. La generazione di un *template* e il momento cruciale del *matching*

Le tecnologie di riconoscimento facciale seguono un percorso scandito da diverse fasi di non sempre agevole ricostruzione.

In primo luogo, ai fini dello svolgimento della procedura è necessaria l'acquisizione dell'immagine che ritrae il volto del soggetto di interesse, in formato digitale, attraverso uno scatto fotografico, o tramite una ripresa video[103]. Il campione biometrico ottenuto è contenuto all'interno di un *file*, le cui dimensioni sono variabili.

In questo ambito occorre evidenziare che l'apprensione dell'immagine del volto avviene raramente con il contributo attivo da parte della persona interessata e più frequente è l'uso di immagini ricavate in ambienti non controllati.

Segue poi una fase più tecnica volta all'individuazione e all'isolamento del volto rispetto all'ambiente circostante[104]. Tale operazione risulta essere particolarmente complessa qualora l'immagine provenga da sistemi biometrici passivi, in ambienti non controllati, in ragione della tendenziale scarsa qualità delle immagini e del posizionamento spesso sfavorevole del soggetto rispetto all'obiettivo[105]. A tale operazione segue la c.d. normalizzazione che ha lo scopo di uniformare le regioni del volto. È in questa fase che l'operatore procede al ridimensionamento dell'immagine, alla sua rotazione o all'allineamento della distribuzione del colore[106]. Rientra all'interno della fase di normalizzazione anche l'individuazione di quelli che vengono definiti "*landmarks*" idonei ad evidenziare i tratti tipici del volto della persona, quali il contorno del viso, i

---

[101] FRA – European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, (p. 7)
[102] *Ibidem*
[103] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 32) nello stesso senso anche Gruppo di lavoro Articolo 29 per la protezione dei dati, in *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobili*, 22/03/2012, (p. 2)
[104] *Ibidem*
[105] *Ibidem*
[106] *Ibidem*

lineamenti delle labbra, la forma del naso o la posizione degli occhi[107]. Una tale operazione, analogamente a quanto si è detto rispetto a quella di isolamento del volto, può risultare particolarmente complessa: le regioni del viso potrebbero, infatti, risultare disomogenee a causa della posizione assunta dall'individuo o della carente luminosità della stanza.

Successivamente il sistema procede all'estrazione delle "caratteristiche biometriche distintive e riproducibili dell'immagine digitale del volto"[108]. Questa fase può avvenire seguendo tre diverse modalità. È possibile procedere riproducendo digitalmente l'intero volto, muovendosi dunque in modo olistico, oppure atomisticamente concentrandosi su specifici tratti biometrici. Talvolta è invece preferibile seguire una modalità mista che ricomprenda entrambi i metodi[109].

Al termine di queste procedure il sistema converte le caratteristiche essenziali processate preventivamente in un "modello biometrico di riferimento", ossia un'immagine vettoriale nominata *template* biometrico[110].

Una volta che sia stato generato il modello biometrico facciale, è possibile procedere all'interrogazione vera e propria del sistema di riconoscimento. Pertanto, il *template* verrà confrontato con quelli presenti all'interno della *watchlist* di riferimento, o del *database* utilizzato. Successivamente, il sistema potrà restituire come *output* un segnale di *alert*, qualora vi sia stato un *match;* il confronto sarà dunque concluso positivamente riscontrando una somiglianza tra l'immagine sottoposta ad analisi ed una già presente nella banca dati.

---

[107] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 33) nello stesso senso anche Gruppo di lavoro Articolo 29 per la protezione dei dati, in *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobili*, 22/03/2012, (p. 2)

[108] *Ibidem*

[109] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 33)

[110] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 33) nello stesso senso anche Gruppo di lavoro Articolo 29 per la protezione dei dati, in *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobili*, 22/03/2012, (p. 2)

2.1.2. Quando non fila tutto liscio: tra falsi-positivi, falsi-negativi e *bias*

I calcoli effettuati dal *software* hanno natura prettamente probabilistica. Ne consegue che essi subiscono necessariamente un margine di errore. Si tratta di un problema non marginale, se si considera che le informazioni raccolte grazie a tali strumenti sono suscettibili di essere impiegate nel procedimento penale. In concreto, potrà darsi sia un falso-positivo, sia un falso-negativo.

Si ottiene un falso-positivo quando il sistema restituisce un *alert* in conseguenza di un *match* errato. Questo comporta la falsa identificazione di un soggetto all'interno della *watchlist* che potrebbe indurre le forze di polizia ad orientare le indagini nei confronti di un sospettato sbagliato, con evidenti ricadute sui diritti fondamentali di quest'ultimo.

Diversamente si verifica un falso-negativo in tutte le circostanze in cui l'algoritmo non è in grado di rilevare la corrispondenza tra due immagini che rappresenterebbero, al contrario, la stessa persona. Conseguentemente l'operatore non riceverebbe alcun segnale di *alert* e non darebbe luogo agli accertamenti dovuti sulla persona.

Il verificarsi di tali tipologie di errori dipende da molteplici fattori, fra i quali l'utilizzo di strumentazione inidonea all'ottenimento di immagini che rispettino lo standard qualitativo richiesto per poter eseguire efficacemente il riconoscimento del volto[111]. Si pensi, ad esempio, alla videocamera di sorveglianza posta all'entrata di un negozio, che spesso restituisce immagini di scarsa qualità.

Ad incidere negativamente il risultato possono concorrere anche fattori prettamente fisici della persona ritratta, come il colore della pelle, che può rendere difficile la fase di "individuazione del volto", specialmente nell'ipotesi in cui l'immagine a disposizione per il riconoscimento sia stata appresa in un luogo eccessivamente luminoso o buio, rendendo la distinzione tra il volto e lo sfondo quasi impossibile[112]. Ancora, l'immagine di una persona pesantemente truccata potrebbe falsare la rilevazione di alcune caratteristiche fondamentali del suo volto[113].

---

[111] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 36)
[112] *Ibidem*
[113] *Ibidem*

Un ulteriore fattore che va preso in considerazione è rappresentato dalla sensibilità propria del sistema, da intendersi come la minima variazione rilevabile dal *software* che determina un *trade-off* tra falsi-positivi e falsi-negativi[114]. In particolare, maggiore è la sensibilità del sistema, minore sarà la possibilità che si verifichino falsi-positivi. L'algoritmo sarà più incline a considerare con maggior accuratezza la coincidenza delle immagini e, conseguentemente, la probabilità di ottenere un falso-negativo sarà più elevata. Tale sarebbe l'effetto diretto dell'incapacità del sistema di riconoscere una corrispondenza quando le immagini, seppur ritraenti lo stesso soggetto, siano eccessivamente diverse[115]. Si tratta però di una caratteristica variabile del *software*, perché in base alla sensibilità definita in fase di programmazione il rendimento della tecnologia varia.
In particolare, la sensibilità varierà in base alle necessità e agli scopi per i quali l'algoritmo deve essere impiegato. Appare dunque implicito che nel contesto dell'utilizzo della tecnologia di riconoscimento facciale per finalità di *law enforcement* è auspicabile l'impostazione di un tasso di sensibilità che garantisca una percentuale minima di errore.

Vi è poi un problema che si pone, per così dire, a monte. Trattandosi infatti di una tecnologia che sfrutta la tecnica di *machine learning,* l'output è influenzato anche dai dati e dai modelli biometrici utilizzati in fase di *training*. Le problematiche maggiori si verificano nel caso in cui la predetta fase si sviluppi sulla base di principi ed ideologie discriminatorie, che portano, per esempio, a sottoporre all'algoritmo in misura maggiore immagini ritraenti persone appartenenti a specifici gruppi etnici piuttosto che un *range* eterogeneo di individui. Il rischio che il *software* elabori i dati in maniera discriminatoria può riguardare caratteristiche ulteriori, come l'età o il sesso, riverberandosi anche su determinate categorie di soggetti, come quelli affetti da forme di disabilità[116].

---

[114] *Ibidem.*
Nello stesso senso anche FRA – European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, (p. 9)
[115] *Ibidem*
[116] FRA – European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, (p. 10)

In queste circostanze si configurerebbe il c.d. effetto "*garbage in, garbage out*"[117], in base al quale l'utilizzo di dati viziati o di bassa qualità all'interno di un algoritmo non può che portare all'ottenimento di *output* altrettanto scadenti o discriminatori. Emergono, sotto questo profilo, i limiti propri dei sistemi di intelligenza artificiale, i quali possono operare solo in base alle informazioni fornitegli dagli operatori.

È dunque essenziale che venga importato nel *software* un *set* di dati di *training* accurato e di qualità, privo di fattori discriminanti, nel rispetto del principio di accuratezza sancito all'art. 5 co. 1 lett. d) Regolamento 2016/679/UE in base al quale i dati personali devono essere "esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati".

2.1.3. L'impatto dell'uso degli strumenti biometrici sull'opinione pubblica

Analizzate sotto il profilo tecnico le potenzialità offerte da questa strumentazione, appare importante soffermarsi su come viene percepito il suo utilizzo da parte dell'opinione pubblica. Occorre chiedersi fino a che punto il cittadino è disposto a sacrificare le proprie libertà e le sue fondamentali facoltà in nome dell'esigenza di sentirsi al sicuro nella propria vita quotidiana e nelle proprie relazioni interpersonali.

È proprio in questa direzione che si è mossa l'indagine svolta da parte della "*European Union Agency for Fundamental Rights*" (FRA) nel 2015[118]. Il sondaggio ha considerato l'opinione di 1227 cittadini di diverse nazionalità, che si accingevano a varcare il confine fra Stati in sette valichi di frontiera diversi[119]. I risultati ottenuti sono stati per la maggior parte di natura negativa e contraria: il 26% ha ritenuto umiliante fornire la propria immagine del volto, il 18% lo ha percepito come una estrema invasione della propria *privacy* e il 12% ha affermato di sentirsi particolarmente a disagio[120]. Diversamente, il

---

[117] C. GARVIE, *Garbage in, Garbage out. Face recognition in flawed data*, 16/05/2019 in https://www.flawedfacedata.com/ consultato il 18/07/2023

[118] FRA – European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, (p. 18)

[119] *Ibidem*

[120] *Ibidem*

38% degli intervistati[121], ha ritenuto non eccessivamente invasiva la richiesta di presentare un documento ritraente il proprio volto per poter oltrepassare il confine, considerando tale procedura necessaria per garantire un adeguato livello di sicurezza pubblica.

Simili risultati sono stati ottenuti anche attraverso un sondaggio condotto in territorio francese, a Nizza, sull'utilizzo della tecnologia di riconoscimento facciale in modalità *live* con una percentuale esigua del 3% di voti sfavorevoli[122].

Parimenti uno studio condotto dall' "*Ada Lovelace Institute*" nel 2019 nel Regno Unito[123] riporta che soltanto il 9% della popolazione risente dell'utilizzo dei sistemi di riconoscimento facciale da parte della polizia e solo il 10% si sente a disagio quando la stessa è utilizzata negli aeroporti[124].

Ciò che è possibile desumere dai risultati riportati è che il sentimento più diffuso sia quello di maggior sicurezza e fiducia quando la tecnologia *de quo* viene sfruttata per finalità di *law enforcement*, nonostante permanga comunque, seppur in misura minore, un'opinione contraria nella maggior parte dei casi sorretta da un'esigenza di maggior riservatezza e tutela della propria *privacy*[125].

Cionondimeno è da considerarsi il momento storico attuale caratterizzato ormai da decenni da un'evoluzione tecnologica dirompente, agli albori inimmaginabile. Viviamo ad oggi in quella che è stata definita dall'informatico John Mashey come "epoca dei *big data*" madre del fenomeno di "datificazione" che trasforma la vita di ciascuno di noi in dati preziosi, a tal punto da assumere valore economico. In sostanza, tutto ciò che facciamo nella nostra quotidianità è suscettibile di assumere valore numerico e ciò ha portato la *Cybersfera* negli anni a rappresentare uno "spazio pubblico accessibile a chiunque, continuamente in espansione e nel quale ognuno (sia esso un soggetto pubblico

---

[121] *Ibidem*
[122] FRA – European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, (p. 19)
[123] Ada Lovelace Institute, *Beyond face value: public attitudes to facial recognition technology*, 2019, https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/ consultato il 19/07/2023
[124] FRA – European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, (p. 19)
[125] FRA – European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, (p. 19 ss)

o privato) riversa inarrestabilmente dati che lo riguardano, attraverso strumenti che lo accompagnano in ogni momento della sua giornata"[126]. Questa tendenza può evidentemente tradursi in occasioni di "sorveglianza digitale di massa"[127] da parte delle autorità che, inevitabilmente, determinano malumori nell'opinione pubblica. In questo, le persone non solo vengono messe sotto la lente di ingrandimento, ma vengono anche costrette (spesso in modo inconsapevole) a mutare la propria personalità e il loro agire quotidiano[128].

2.2. Tecnologie di riconoscimento facciale e protezione dei diritti fondamentali

2.2.1. Il problema dell'impatto sui diritti fondamentali e lo scorcio dello "*human-in-the-loop*"

Il timore per la violazione dei diritti fondamentali degli interessati è un caposaldo su cui si muove la Commissione Europea all'interno del *Libro Bianco sull'Intelligenza Artificiale* stilato nel 2020. Le tecnologie di riconoscimento facciale sono ad oggi in grado di analizzare una quantità smisurata di dati riferiti in maniera diretta a persone fisiche identificate o identificabili, soprattutto quando operano in modalità *real time*; pertanto, è indubbio il rischio che queste siano idonee ad arrecare pregiudizio ai soggetti interessati.

Primo diritto che è suscettibile di subire una sua compressione per effetto dell'utilizzo di questi sistemi è il diritto al rispetto della vita privata e alla protezione dei dati personali. "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa

[126] C. SARRA, *Il mondo-dato. Saggi su datificazione e diritto,* 2019, (p. 32)
[127] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 78)
[128] *Ibidem*

dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui" (art. 7 Carta dei diritti fondamentali dell'Unione Europea)[129]. Le tecnologie di riconoscimento facciale determinano una significativa intrusione nella sfera privata di ciascun cittadino sotto diversi punti di vista.

La principale violazione al diritto alla *privacy* è determinata dalla totale assenza, in Italia, di una legge che disciplini in maniera specifica questa tipologia di strumentazioni, la quale comporta l'illegittimità delle intrusioni da esse determinate.

Si pensi poi alla tipologia di dati di cui si servono gli algoritmi in questione. Si tratta di dati in grado di consentire l'identificazione di una persona fisica, che di regola, non dovrebbero essere oggetto di trattamento, se non in specifici casi di deroga, fra i quali rientrano proprio le esigenze di pubblica sicurezza. Eppure, nonostante il carattere di estrema sensibilità dei dati analizzati la maggior parte delle operazioni di identificazione avviene in maniera occulta, senza il previo consenso degli interessati[130]. L'interessato perde del tutto il controllo sulla circolazione dei dati che lo riguardano, subendo in questo modo anche una lesione del suo diritto all'autodeterminazione. Qualora sia svolta in segreto, l'attività di riconoscimento impedisce infatti alla persona di autodeterminarsi sui dati e le informazioni che la riguardano. In questo modo, la facoltà di "decidere, in autonomia e consapevolmente, in che modo le informazioni che lo riguardano siano acquisite e conservate"[131] viene totalmente vanificata. La violazione di quest'ultimo diritto comporta un'inosservanza anche del Regolamento europeo 2016/679, ove sancisce che, in tutti i casi in cui i dati non siano forniti dall'interessato, il titolare del trattamento è ulteriormente tenuto a fornire "informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato"[132], comunicazioni che ovviamente è improbabile l'Autorità fornisca, ove manchi a priori il consenso dell'interessato[133].

---

[129] Analogamente anche art. 8 Convenzione Europea dei Diritti dell'Uomo

[130] E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Diritto Penale e Uomo*, Milano, fascicolo 5/2021, (p. 78)

[131] E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Diritto Penale e Uomo*, Milano, fascicolo 5/2021, (p. 79)

[132] Dispositivo dell'art. 14 comma 2 lettera g) GDPR

[133] *Ibidem*

Non meno vulnerate risultano la libertà di espressione e associazione, capisaldi all'interno di una società democratica e tutelati sia a livello europeo che costituzionale[134]. Appare evidente che, ad esempio, l'utilizzo di tecnologie di riconoscimento facciale in modalità sincrona durante manifestazioni pubbliche per i diritti civili può trasformarsi in una occasione di repressione la cui conseguenza diretta è il già citato *chilling effect*[135]. Il cittadino si sentirebbe minacciato dalla presenza di una videocamera in grado di acquisire e conservare migliaia di fotogrammi che lo ritraggono in tali peculiari circostanze e potrebbe trovarsi costretto a rinunciare alla propria libertà di manifestazione del pensiero, temendo future ripercussioni.

Inoltre, poiché i dati raccolti e le identità disvelate attraverso questi strumenti sono elementi utili per il procedimento penale, consentendone, ad esempio, l'avvio o, ancor prima, permettendo l'applicazione di misure preventive limitative della libertà personale[136], viene in gioco il problema della compatibilità dell'impiego delle tecnologie di riconoscimento facciale con il diritto alla tutela giurisdizionale e all'equo processo. La Costituzione garantisce la possibilità di agire in giudizio ai fini della tutela dei propri diritti e interessi legittimi (art. 24 Cost.) nel rispetto delle garanzie del giusto processo, tra le quali spicca il contradditorio nella formazione della prova (art. 111 Cost.). La natura opaca dei sistemi di intelligenza artificiale sembra contraria al dettato costituzionale in ragione della sostanziale impossibilità di poter verificare il procedimento seguito dall'algoritmo in fase di esecuzione, di cui nemmeno gli operatori hanno il pieno controllo. Ne consegue che il soggetto risulta privo di strumenti per difendersi nel processo di fronte all'utilizzo di un meccanismo di cui è ignoto il funzionamento, non essendo possibile contestare le procedure che hanno condotto ad un esito sicuramente pregiudizievole per le garanzie di cui è titolare[137].

---

[134] Art. 11 Carta dei diritti fondamentali dell'Unione Europea, Art. 21 Costituzione italiana, Art. 18 Costituzione italiana

[135] E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Diritto Penale e Uomo*, Milano, fascicolo 5/2021, (p. 80)

[136] E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Diritto Penale e Uomo*, Milano, fascicolo 5/2021, (p. 79 ss)

[137] E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Diritto Penale e Uomo*, Milano, fascicolo 5/2021, (p. 80)

Parimenti, l'impenetrabilità della *black box* algoritmica dei moderni sistemi di intelligenza artificiale rende impraticabile anche l'esercizio del diritto di accesso riconosciuto in capo all'interessato del trattamento dall'art. 15 del Regolamento europeo 2016/679. Lo stesso garantirebbe, infatti, al titolare dei dati di poter accedere a questi ultimi ed essere informato circa le finalità del trattamento, le categorie di dati personali trattate, i destinatari dei dati, il periodo di conservazione ed, in particolare, dell'esistenza di un processo decisionale automatizzato su di questi.

Per la verità, il problema dell'impenetrabilità dell'algoritmo sembra poter essere attenuato (anche se non del tutto superato) dall'obbligo di un intervento umano sull'*output* elaborato dal sistema. Spetterebbe infatti all'operatore umano il compito di dare conferma o meno del risultato ottenuto "applicando le procedure di comparazione fisionomica, rispetto alle quali le forze di polizia scientifica ricevono una specifica formazione"[138]. Nel rispetto del dettato normativo europeo, infatti, l'ammissibilità di una decisione basata unicamente su un trattamento automatizzato, idonea a produrre effetti giuridici negativi o ad incidere in maniera significativa sull'interessato, deve ravvisarsi, oltre che sulla predisposizione di una idonea base normativa, anche sulla possibilità per il titolare dei dati di ottenere l'intervento umano da parte del titolare del trattamento[139]. In conclusione, non si tratta di una misura in grado di escludere totalmente il rischio di erronee identificazioni. Considerando infatti quanto in precedenza detto in merito all'inesplicabilità umana di alcuni calcoli eseguiti dagli algoritmi, risulterebbe irrealistico poterne dominare gli *output*. Tuttavia, pare comunque una previsione in grado di garantire il rispetto del principio dello *human in the loop* (figlio della Direttiva 2016/680/UE) in base al quale si ritiene necessario che l'operatore umano mantenga un ruolo attivo nel processo decisionale eseguito dall'algoritmo, cosicchè sia possibile scongiurare l'assunzione di decisioni basate unicamente su procedure totalmente automatizzate che siano idonee a ledere gli interessi del soggetto che vi si sottopone.

---

[138] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, (p. 33), in *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*. 2022, (p. 33) ed M. VALERI, *Mettiamoci la faccia*, in https://poliziamoderna.poliziadistato.it/articolo/3536228dc7e38a89165859531 9 marzo 2022, consultato il 22/07/2023

[139] Dispositivo dell'art. 11 Direttiva 2016/680/UE

2.2.2. La tutela delle categorie di soggetti più deboli

I problemi sinora evidenziati si enfatizzano se i destinatari del trattamento sono soggetti deboli, come bambini, anziani o persone con disabilità, verso cui, da sempre, il nostro legislatore appresta una tutela particolare.

Ci si interroga in particolare sulla necessità di tutelare il minore di fronte all'utilizzo dei sistemi di riconoscimento facciale in ambienti pubblici come, ad esempio, i valichi di frontiera o le manifestazioni sportive. La stessa *Carta europea dei diritti fondamentali* auspica la protezione del bambino e la salvaguardia del suo primario interesse in tutti gli atti che lo riguardano, compiuti sia da entità pubbliche quanto private[140]. Il legislatore europeo riserva al minore una tutela specifica e rafforzata, dovuta alla sua incapacità di comprendere a pieno i rischi e le conseguenze, oltre che i propri diritti, in relazione al trattamento dei propri dati personali[141]. Inoltre, risulterebbe necessaria una valutazione più ponderata della necessarietà e proporzionalità del trattamento dei dati biometrici[142] soprattutto se si considera la significativa possibilità di errore nell'analisi del modello biometrico di un bambino rispetto a quella effettuata su un adulto. Il volto di una persona in età giovane è soggetto ancora a futuri cambiamenti ed evoluzioni; pertanto, in seguito ad un confronto, sarebbe alquanto probabile ottenere una corrispondenza non affidabile. Va comunque rilevato come le tecnologie di riconoscimento facciale allo stato disponibili siano in grado di operare una valutazione biometrica corretta a partire da immagini del volto, cui età è pari o superiore a sei anni, rapportate ad altre immagini apprese in un lasso temporale minore o uguale a cinque anni rispetto alle prime[143]. Tuttavia, sono da considerarsi in generale mediocri i risultati ottenibili attraverso il riconoscimento facciale di soggetti in età inferiore ai tredici anni, potendosene ricavare per lo più falsi-negativi[144]. Un tale esito potrebbe avere effetti drammatici nella vita di un bambino, si immagini ad esempio il caso in cui il sistema, utilizzato ad una frontiera, non riconosca un minore vittima di rapimento.

---

[140] Dispositivo dell'articolo 24 della Carta dei diritti fondamentali dell'Unione Europea
[141] Enunciazione del considerando 38 del Regolamento europeo 2016/679
[142] FRA – European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, (p. 28)
[143] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, (p. 109)
[144] *Ibidem*

Quanto detto per i minori vale però anche per il caso in cui i soggetti sottoposti al trattamento siano anziani, i cui tratti del volto cambiano rapidamente in età avanzata.

2.2.3. Un'importante pronuncia in materia di utilizzo di tecnologie di riconoscimento facciale: la sentenza della *High Court of Justice* inglese

Non vi sono in Italia pronunce particolarmente significative sulla legittimità dell'impiego degli strumenti di riconoscimento facciale. Pioniera in tal senso è stata la *High Court of Justice* inglese, che ha affrontato direttamente il problema del bilanciamento tra l'utilizzo delle tecnologie in esame da parte degli organi di polizia ed il rispetto dei diritti fondamentali dei cittadini sottoposti al trattamento[145]. In particolare, la Corte è stata chiamata a pronunciarsi sul ricorso proposto dall'attivista inglese Edward Bridges, il quale lamentava l'illegittimo trattamento dei propri dati personali ad opera della polizia inglese, con l'ausilio del *software* "*AFR Locate*", ossia il sistema di riconoscimento facciale in dotazione alle forze dell'ordine britanniche che operava in modalità *live*[146]. Preme sottolineare che, in aggiunta, il signor Bridges non risultava fra i soggetti contenuti all'interno della *watchlist* redatta dall'Autorità, in quanto comune cittadino presente nei luoghi sottoposti a videosorveglianza[147].

I motivi del ricorso erano sostanzialmente tre, tutti respinti dalla Corte.

In primo luogo, la parte attrice sosteneva la violazione dell'articolo 8 CEDU[148] avendo il trattamento dato luogo ad un'illegittima intrusione nella propria vita privata. A tal proposito il giudice ha considerato pacificamente l'effettiva ingerenza nella vita privata del cittadino[149], ma ha ritenuto che tale intrusione non potesse essere ritenuta illegittima, dovendosi constatare che il trattamento rientri tra le prerogative attribuite in capo all'Autorità convenuta per permetterle l'esercizio dei propri poteri[150]. Inoltre,

---

[145] High Court of Justice, Queen's Bench Division, Divisional Court, 4 settembre 2019, Case No: CO/4085/2018, R (Bridges) v. CCSWP e SSHD

[146] J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Diritto penale contemporaneo. Rivista trimestrale*, n. 1/2020, 2020, (p. 236)

[147] [2019] EWHC 2341 (Admin), § 16

[148] [2019] EWHC 2341 (Admin), § 19

[149] [2019] EWHC 2341 (Admin), § 62

[150] [2019] EWHC 2341 (Admin), § 96

l'illegittimità non sarebbe ravvisabile nemmeno con riferimento all'assenza di una base normativa[151]. La Corte ha sostenuto, infatti, che si tratta di strumentazioni rientranti nell'ambito applicativo delle disposizioni a tutela della *privacy*[152], in ragione della presenza, all'interno del *Data Protection Act* del 2018, di una serie di previsioni che possono essere applicate a qualsiasi tipologia di trattamento di dati sensibili posto in essere dalle forze dell'ordine[153]. Ad allargare la base normativa, si aggiungerebbero poi anche altre disposizioni "di rango regolamentare in materia di videosorveglianza[154] e di *local polices*, adottate dalla *South Wales Police*"[155]. Cionondimeno la Corte ha ritenuto opportuno sottolineare che, il trattamento dei dati biometrici facciali, diversamente rispetto a quanto accade per il prelievo del DNA, non implica alcun coinvolgimento fisico diretto con l'interessato; pertanto, si tratterebbe di una fattispecie idonea a ricondursi alla disciplina prevista per le videoriprese[156].

Nel ricorso si lamentava poi la violazione della disciplina interna ed euro unitaria in materia di protezione dei dati personali[157]. Sul punto i giudici hanno, invece, sostenuto la legittimità della finalità perseguita e l'osservanza delle disposizioni specificamente riferite al trattamento di categorie particolari di dati previste dalla normativa[158]. A supporto di tale tesi, la Corte ha sottolineato che il sistema procederebbe a smaltire immediatamente i dati raccolti qualora non si ottenga alcun *match*[159]. In aggiunta, si è considerato il notevole sforzo condotto dalla *South Wales Police* al fine di informare tutti i cittadini della messa in funzione di un tale sistema di intelligenza artificiale, anche attraverso l'utilizzo di piattaforme *social,* quali *Facebook* e *Twitter,* avendo cura di specificarne i luoghi di utilizzo[160]. Allo stesso modo le autorità avrebbero anche provveduto a segnalarne l'impiego, tramite la predisposizione di cartelli segnaletici apposti nei veicoli di ordinanza, presso gli stessi luoghi sottoposti a videosorveglianza[161].

---

[151] [2019] EWHC 2341 (Admin), § 84
[152] [2019] EWHC 2341 (Admin), § 85
[153] J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Diritto penale contemporaneo. Rivista trimestrale*, n. 1/2020, 2020, (p. 237)
[154] Tra le quali il *Surveillance Camera Code of Practice*
[155] *Ibidem*
[156] [2019] EWHC 2341 (Admin), § 74 ss
[157] [2019] EWHC 2341 (Admin), § 20
[158] [2019] EWHC 2341 (Admin), § 122 ss, 133 ss. 139 ss, 144 ss
[159] [2019] EWHC 2341 (Admin), § 37 ss
[160] [2019] EWHC 2341 (Admin), § 39
[161] *Ibidem*

Elemento determinante in questo contesto è stata poi la predisposizione da parte dell'organo di polizia di apposita documentazione atta ad esplicitare il funzionamento del *software* adottato e a delinearne i possibili rischi[162].
Inoltre, con riferimento al potenziale rischio di discriminazione del sistema "*AFR Locate*" nei confronti di donne e talune minoranze etniche[163], si è ritenuto che non fossero state fornite prove a sufficienza per sostenere una tale violazione[164].
Infine, l'adozione da parte della *South Wales Police* di un "*Equality Impact Assessment – Initial Assessment*"[165] e la divulgazione di informazioni circa il tasso di errore riscontrato nel software in fase di collaudo e sua successiva revisione[166] sono stati ritenuti elementi sufficienti per ritenere legittimo l'utilizzo della tecnologia sottoposta a giudizio per finalità di prevenzione e repressione del crimine[167].

Nonostante la sentenza della *High Court of Justice* fornisca innegabilmente molteplici spunti di riflessione e rappresenti una delle prime vere e proprie decisioni in materia di riconoscimento facciale, essa non è stata indenne da critiche. Fra queste, risulta per me essere di particolare rilievo il giudizio espresso dal Garante per la *privacy* inglese (*Information Commissioner's Office*). In particolare, l'autorità garante ha considerato di fondamentale importanza attuare un minuzioso "vaglio di proporzionalità sulla necessità di utilizzare gli strumenti in esame"[168], al fine di tutelare nel modo più assoluto i diritti umani coinvolti nel trattamento. Ritengo, inoltre, come afferma lo stesso ICO, che l'utilizzo di *AFR Locate* non possa essere ammesso pacificamente in assenza di una previsione che espliciti le tipologie di reato alle quali può essere applicato. Per di più, dovrebbero essere considerate soltanto le fattispecie criminose più gravi prevedendo anche l'obbligo, da parte delle autorità, di motivare la scelta di preferire strumentazioni così invasive ad altre.

---

[162] Ci si riferisce al "*Policy on Sensitive Processing for Law Enforcement Purposes*" cfr. [2019] EWHC 2341 (Admin) § 139, ed al "*Data Protection Impact Assesment*" cfr. [2019] EWHC 2341 (Admin) § 147
[163] [2019] EWHC 2341 (Admin), § 20
[164] [2019] EWHC 2341 (Admin), § 153
[165] [2019] EWHC 2341 (Admin), § 158
[166] [2019] EWHC 2341 (Admin), § 154
[167] J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Diritto penale contemporaneo. Rivista trimestrale*, n. 1/2020, 2020, (p. 238)
[168] J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Diritto penale contemporaneo. Rivista trimestrale*, n. 1/2020, 2020, (p. 239)

Tuttavia, nel caso *Bridges*, non sembra essere presente nessuno di questi elementi.
Personalmente, dunque, assumendo un orientamento più garantista, trovo difficile accogliere la pronuncia della Corte, in quanto ritengo che la base normativa inglese sia troppo ridotta e sarebbe, invece, preferibile la predisposizione di una disciplina specifica per l'utilizzo delle tecnologie *de quo*.

2.3. SARI: il caso italiano tra luci ed ombre

Anche l'Italia si è dotata di tecnologie di riconoscimento facciale.
Dal 2017 il "*Sistema Automatico di Riconoscimento delle Immagini*" noto con l'acronimo SARI è in dotazione alle forze dell'ordine italiane, quale risultato degli intensi sforzi compiuti in seno al Ministero degli Interni al fine di dotare le Autorità di una macro-infrastruttura informatica completa in grado di analizzare flussi video ed immagini e permetterne il riconoscimento automatico dei volti in diversi scenari[169]. Parimenti al sistema *AFR* inglese, anche il *software* italiano si compone di due sistemi: *SARI Enterprise* e *SARI Real Time*[170], i quali operano rispettivamente nelle già delineate modalità differita e sincrona.

2.3.1. Sari *Enterprise*

Nella sua declinazione "*Enterprise*" la tecnologia di riconoscimento facciale permette all'operatore di ricostruire l'identità di un individuo, a partire dalla sua immagine facciale. Grazie all'esecuzione di molteplici algoritmi, il sistema sarà in grado di compiere una ricerca automatica all'interno di una banca dati (dell'ordine di 10 milioni di immagini di soggetti preventivamente foto segnalati), ottenendone una lista ordinata di volti simili a quello ritratto in fotografia, in base alla loro similarità[171].

---

[169] Ministero dell'Interno Dipartimento della 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*, (p. 6)
[170] Ministero dell'Interno Dipartimento della 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*, (p. 7)
[171] *Ibidem*

L'operatore ha la possibilità di scegliere all'interno di quale banca dati l'algoritmo deve effettuare la ricerca e quali parametri prendere in considerazione: il volto, i riferimenti anagrafici e descrittivi delle fotografie contenute nella banca dati di riferimento; ma egli può anche combinare le precedenti modalità di ricerca.
Il sistema *Enterprise* sfrutta in particolare il *database* AFIS, e parallelamente SSA, già ampiamente in uso dalle forze dell'ordine, al cui interno vengono conservate più di 17 mila immagini segnaletiche[172][173].
Al termine della ricerca il sistema restituisce un elenco di cinquanta o più immagini facciali simili a quella ricercata, ma rimane sempre in capo all'operatore umano il compito di verificare quale fra i volti presenti rappresenta maggiormente quello dell'interessato[174].

In merito a tale applicativo si è espresso il Garante per la Protezione dei Dati Personali, nel provvedimento n. 440 del 26 luglio 2018. In particolare, la componente *Enterprise* consentirebbe la mera automatizzazione di talune operazioni che, precedentemente al suo utilizzo, richiedevano il meccanico inserimento da parte dell'operatore umano dei connotati identificativi dell'interessato[175]. L'utente sarebbe così agevolato, dovendo procedere all'inserimento dell'immagine ritraente il volto della persona di interesse nell'archivio dei soggetti fotosegnalati[176]. Questo permetterebbe l'avvio della ricerca e l'automatica elaborazione dei dati da parte dell'algoritmo per la generazione della lista di corrispondenza. In sostanza, ritiene il Garante, SARI *Enterprise* non darebbe luogo ad un

---

[172] AFIS è l'acronimo di "Automated Fingerprint Identification System". All'interno di tale archivio sono memorizzati tutti i cartellini foto-segnaletici redatti dalle forze dell'ordine e, più specificatamente, immagini delle impronte digitali e dati anagrafici e biometrici di tutti i soggetti sottoposti a rilievi.
SSA indica, invece, l'applicazione *web-based* utilizzata dalle autorità "per la gestione e la ricerca dell'identità di un soggetto sconosciuto all'interno della banca dati dei soggetti fotosegnalati".
Cit. Ministero dell'Interno Dipartimento della 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*, (p. 10)
[173] Ministero dell'Interno, *Interrogazione parlamentare n. 3-02074*, https://www.camera.it/leg18/410?idSeduta=0463&tipo=stenografico consultato il 24/07/2023
[174] Ministero dell'Interno Dipartimento della 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*, (p. 26)
[175] Garante per la Protezione dei Dati Personali, *provvedimento n. 440 del 26/07/2018*, doc. web n. 9040256, consultato in data 24/07/2023
[176] *Ibidem*

trattamento di dati personali *ex novo*, ma costituirebbe altresì una "nuova modalità di trattamento di dati biometrici"[177].

La legittimità del trattamento operato dal sistema *Enterprise* sarebbe ravvisabile sotto diversi punti di vista. In primo luogo, esso rientrerebbe nell'alveo dei trattamenti di dati personali elettronici previsti nel Decreto del Ministero dell'Interno siglato il 24 maggio 2017 sotto la denominazione "Sistema A.F.I.S. (*Automated Fingerprint Identification System*). *Identificazione personale*". In particolare, la scheda n. 19 di tale documento riporta una consistente elencazione di fonti normative e relative misure volte a garantire il rispetto dei diritti fondamentali dei soggetti coinvolti, dovendosi così ritenere soddisfatta la previsione dell'art. 7 d.Lgs. 18 maggio 2018 n. 51.

In egual misura, non sarebbe ravvisabile nemmeno una violazione dell'art. 8 che vieta le decisioni basate su un trattamento unicamente automatizzato in grado di produrre effetti lesivi nei confronti dell'interessato. Il trattamento è in questo caso legittimo in ragione dell'apporto umano decisivo sull'elaborazione della macchina, idoneo ad individuare la corrispondenza più appropriata tra quelle proposte.

In conclusione, dunque, è da considerare positivo il parere espresso dal Garante circa l'impiego della componente *Enterprise*.

Nonostante ciò, i pareri discordanti non sono stati messi a tacere. Tuttavia, per quel che mi riguarda, condivido la posizione espressa nella sua quasi totalità.

A generare in me ancora qualche cenno di esitazione sono le sproporzioni che caratterizzano il contenuto del *database* utilizzato dal sistema per il riconoscimento. In particolare, si noti che in una banca dati composta da circa 10 milioni di immagini, 2 milioni apparterrebbero a cittadini italiani, mentre i restanti 7 milioni ritrarrebbero persone straniere[178]. Una tale disomogeneità rischia in effetti di condannare SARI a tecnologia discriminatoria e quindi illegittima. Il problema maggiore si verifica al momento dell'addestramento dell'algoritmo. Infatti, sfruttando tecniche di *machine learning*, qualora il *set* di dati di *training* fosse costituito prevalentemente da uomini neri,

---

[177] *Ibidem*

[178] ANGIUS, R., & COLUCCINI, R. (a cura di) (2019) *Riconoscimento facciale, nel database di Sari quasi 8 schedati su 10 sono stranieri.* https://www.wired.it/attualita/tech/2019/04/03/sari-riconoscimento-facciale-stranieri/ consultato il 23/09/2023

nel caso in cui l'algoritmo dovesse riconoscere persone di genere diverso o con un altro colore della pelle, il rischio di ottenere un *output* errato aumenterebbe[179]. Il pericolo in questo caso è quello di dar luogo a controlli, da parte delle forze dell'ordine, sulle persone sbagliate.

Pertanto, a mio parere, SARI *Enterprise* potrebbe essere reso disponibile alle autorità soltanto una volta che il database di allenamento sia stato attentamente valutato e reso quanto più eterogeneo possibile.

2.3.2. Sari *Real Time*

La componente *Real Time* presenta funzionalità tecnicamente più avanzate ed avveniristiche rispetto alla precedente. In effetti, la modalità *Real Time* avrebbe raggio applicativo ben più ampio, potenzialmente indiscriminato, potendosi impiegare in aree geografiche ove siano posizionate videocamere di sorveglianza idonee a consentire l'apprensione di flussi video che, una volta sottoposti al sistema di riconoscimento, permettano l'individuazione dei volti che vi compaiono. Le immagini facciali apprese vengono confrontate con la *watchlist*, dell'ordine di 100.000 soggetti, stilata dagli operatori e confrontate con le immagini ivi presenti, generando un segnale di *alert* quando il sistema abbia individuato un *match*[180]. Tale sistema permetterebbe la sorveglianza di aree particolarmente affollate, quali ad esempio stadi, manifestazioni pubbliche, piazze in cui vi sia il concreto rischio che si verifichino disordini, rivolte o attentati.

Le criticità che riguardano la procedura *de quo*, per le quali è stato richiesto l'intervento del Garante sulla sua utilizzabilità, muovono principalmente dall'ampiezza del *set* di dati sensibili che vengono ad essere analizzati in maniera indiscriminata. In ragione delle peculiarità di un tale trattamento, il Garante ha ritenuto di esprimere un parere al riguardo. In particolare, si è sostenuto che, qualora il sistema operi in modalità sincrona, esso realizza il trattamento su larga scala di dati biometrici, senza distinguere tra soggetti inseriti nella *watchlist* e comuni cittadini presenti nel luogo di interesse, determinandosi

---

[179] *Ibidem*

[180] Ministero dell'Interno Dipartimento della 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*, (p. 7)

così un'occasione di sorveglianza di massa[181]. Una tale ingerenza nella vita privata di ciascun individuo video-ripreso determina obbligatoriamente la predisposizione di una specifica base normativa che consenta l'utilizzo di tali tecnologie come richiesto dagli artt. 7 d.Lgs. 51/2018 e 8 CEDU.

Il Garante ha rilevato la mancanza di una tale base sia a livello interno, sia a livello europeo. In particolare, il d.Lgs. 51/2018 non specifica i presupposti in base ai quali può ritenersi legittimo l'impiego della tecnologia SARI *Real Time*[182]. Né se ne può giustificare l'utilizzo in base ad altre previsioni, come, ad esempio l'art. 1 T.U.L.P.S., che non contiene alcun riferimento al trattamento in esame[183].

Risulta, pertanto, imprescindibile l'elaborazione di una disciplina specifica, che indichi per quali fattispecie può essere applicato tale *software* e quali garanzie ne presidiano l'utilizzo[184].

Inoltre, anche l'assoluta inconoscibilità, allo stato, dei criteri che determinano la stesura della *watchlist*, o quelli relativi alla individuazione delle circostanze in cui il sistema deve essere applicato portano a ritenere sempre illegittimo l'impiego di questa tecnologia nella sua forma *Real Time*[185]. Manca poi una strategia informativa nazionale circa l'utilizzo della stessa. A differenza di quanto è accaduto con il *software* AFR inglese, le autorità italiane infatti non hanno provveduto a dare notizia dell'imminente uso di SARI *Real Time* attraverso piattaforme *social* o, comunque, attraverso altri canali informativi che potessero garantire un avviso su larga scala[186]. Va, infine, rilevato come non sia nemmeno possibile avere indicazioni relative al tasso di errore del sistema e, quindi, alla quantità di false identificazioni e possibili discriminazioni effettuate dall'algoritmo, né specularmente circa la *performance* positiva di tale tecnologia[187].

---

[181] Garante per la Protezione dei Dati Personali, *parere n. 127 del 25/03/2021*, doc. web n. 9575877, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877 consultato in data 24/07/2023

[182] *Ibidem*

[183] *Ibidem*

[184] *Ibidem*

[185] *Ibidem*

[186] J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Diritto penale contemporaneo. Rivista trimestrale*, n. 1/2020, 2020, (p. 242)

[187] J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Diritto penale contemporaneo. Rivista trimestrale*, n. 1/2020, 2020, (p. 243)

In sostanza, è possibile affermare pacificamente la totale inosservanza del fondamentale principio di trasparenza, al quale dovrebbe conformarsi il trattamento dei dati[188].

Ad oggi, dunque, risulta fallito il tentativo di introdurre un sistema così invasivo. Per consentirne in futuro l'impiego per la prevenzione e la repressione dei reati è indispensabile procedere ad un suo perfezionamento, tenendo presenti le indicazioni del Garante.

[188] *Ibidem*

Capitolo III

Conclusioni

Il caso inglese e quello italiano sono soltanto due esempi dei molteplici tentativi di introdurre e disciplinare i sistemi di riconoscimento facciale a livello interno e sovranazionale.

Rimanendo in territorio europeo, la stessa Unione Europea, parallelamente all'adozione della Convenzione Schengen, ha provveduto allo sviluppo del "Sistema d'Informazione Schengen" (SIS), la cui finalità in prima battuta mirava a sopperire all'assenza di barriere fisiche interne nello spazio Schengen. Il raggiungimento di tale obbiettivo avveniva preservando l'ordine e la sicurezza pubblica, compresa la sicurezza dello Stato e assicurando l'applicazione, nel territorio delle Parti contraenti delle disposizioni sulla circolazione delle persone stabilite nella Convenzione Schengen[189]. Tuttavia, le ondate terroristiche dei primi anni duemila hanno reso necessario procedere ad un *upgrade* del sistema a SIS II, il quale mira ad un più ampio scopo di tutela della sicurezza pubblica interna degli Stati parte dell'area, prevedendo la possibilità di condivisione fra le autorità di informazioni e dati di tipo biometrico riferiti ad una platea indeterminata di persone fisiche possibili sospettate, anche a fini preventivi[190].

Funzionano in modo simile i sistemi EURODAC[191], VIS[192] e EES[193], che conservano anch'essi dati biometrici come impronte digitali e immagini facciali. Si tratta, però, di sistemi il cui utilizzo deve intendersi localizzato presso i valichi di frontiera e non tanto nell'ambito di pubbliche manifestazioni. Inoltre, preme sottolineare che, mentre a livello europeo l'introduzione di apparati di una tale entità è stata accompagnata e sorretta da un'idonea ed efficace regolamentazione con forti basi normative, non è possibile affermare lo stesso in ambito interno, quantomeno in Italia.

---

[189] Dispositivo dell'art. 93 Convenzione Schengen

[190] A. BALDACCINI, *Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases*, in *European Journal of Migration and Law*, 2008, (p. 37 ss)

[191] Acronimo di "*European Asylum Dactyloscopie Database*", ossia il sistema europeo per il confronto delle impronte digitali dei richiedenti asilo

[192] Acronimo di "Sistema di Informazione Visti", ovvero un sistema informatizzato di condivisione di dati relativi ai visti d'ingresso nello Spazio Schengen tra gli Stati che ne fanno parte

[193] Acronimo di "*Entry/Exit System*", ovvero un sistema di gestione delle frontiere esterne Schengen

A valle delle considerazioni fintanto esposte si osserva che le tecnologie di riconoscimento facciale, pur essendo state accolte più che positivamente da parte degli organi di polizia, in ragione della loro capacità di assurgere a strumento di ausilio straordinario alle proprie mansioni, presentino notevoli criticità. A spaventare in misura maggiore è probabilmente la possibilità offerta dai sistemi di riconoscimento di dar luogo ad occasioni di vera e propria sorveglianza di massa. Rappresentazione più concreta e angosciante di questo futuro distopico è la realtà cinese. È ormai nota l'introduzione da parte del governo di quel Paese del "Sistema di Credito Sociale". Si tratta di un sistema che vorrebbe incentivare le "buone azioni" da parte dei cittadini e delle imprese, attribuendo loro dei crediti e sottraendoli, qualora il loro comportamento sociale non sia ritenuto idoneo e coerente all'ideologia del Partito. L'idea nasce dalla possibilità di sfruttare i *big data* per monitorare e controllare la popolazione[194]. Carattere fondamentale di questo progetto è la previsione di un sistema di ricompense e punizioni organizzato per mezzo di liste, rispettivamente rosse e nere. L'iscrizione nell'una o nell'altra lista determina importanti conseguenze su più fronti. Si pensi, ad esempio, alla riduzione delle contribuzioni fiscali dovute, o, in caso di inserimenti nella *black list* una minor probabilità di ottenere l'approvazione dell'autorità per il compimento di specifiche attività[195]. Tuttavia, i criteri che influiscono sull'iscrizione ad una lista piuttosto che ad un'altra non sono attualmente di pubblico dominio, comportando pertanto la tendenza da parte delle imprese e dei cittadini ad attenersi alle regole prestabilite per non imbattersi in situazioni particolarmente sfavorevoli.

Il *software* impiegato dal governo cinese presenta poi profili discriminatori. Tale strumento è in grado di riconoscere i volti dei cittadini e distinguerli in base alla loro etnia, catalogando e memorizzando i dati biometrici direttamente riferibili ai soggetti appartenenti a minoranze, come, ad esempio, i musulmani uiguri. Ciò sarebbe possibile grazie all'installazione, in tutto il territorio occidentale dello Xijiang di videocamere di sorveglianza in grado di identificare gli individui e riprenderli nelle proprie attività quotidiane.

---

[194] L. LIN e C. MILHAUPT, *China's Corporate Social Credit System and the Dawn of Surveillance State Capitalism*, in *The China Quarterly,* 2023, (p. 4)
[195] *Ibidem*

Evidentemente un tale strumento, inserito all'interno della realtà politico-sociale cinese, rischia effettivamente di diventare un mezzo di censura ed emarginazione sociale dalla quale difficilmente è possibile tornare indietro[196].

Malgrado la drammaticità della situazione cinese, è quanto mai imperativo sottolineare il carattere profondamente diverso del contesto europeo. La forte componente autoritaria della forma di governo di quel Paese ostacola l'adeguata tutela dei diritti individuali e della libertà personale di ciascun cittadino.
Diversamente, in ambito europeo il legislatore ha adottato un'impostazione normativa largamente rispettosa dei diritti fondamentali dell'uomo, dimostrando anche una profonda preoccupazione verso la materia dei dati personali, come testimonia l'entrata in vigore del Regolamento 2016/679/UE.
Tuttavia, il riferimento al caso cinese non ha una rilevanza meramente teorica, ma deve costituire un monito. In considerazione delle criticità che si sono evidenziate, occorre discostarsene nettamente. Le tecnologie di riconoscimento facciale nella società odierna vanno introdotte con cautela, prestando particolare attenzione alla loro regolamentazione.

Per concludere, l'implementazione delle tecnologie in grado di riconoscere automaticamente il volto di una persona e di attribuirle un'identità trova ad oggi un percorso irto di ostacoli.
A pesare è soprattutto il timore di un impiego abusivo dei dati personali, in particolare di tipo biometrico. Il sentimento di impotenza e scarsa governabilità del procedimento rende l'individuo vulnerabile di fronte ad una realtà che lo costringe a mostrare il proprio volto, senza potersi nascondere, determinandosi così una lesione alla propria *privacy*.
Il rischio è che l'utilizzo indiscriminato e privo di ogni limite normativo di una tale tecnologia porti alla fondazione di società in cui le persone percepiscano di essere costantemente sotto stretta osservazione perché sospettate, invece di sentirsi libere[197]. Si

---

[196] GUZZONATO, C. (a cura di) (2022) *Che cos'è e come funziona il sistema di credito sociale in Cina*. https://www.focus.it/tecnologia/digital-life/cos-e-e-come-funziona-il-sistema-di-credito-sociale-cinese consultato il 10/08/2023
[197] F. I. GAROFOLI, *Il rischio inquisitorio negli strumenti di intelligenza artificiale*, in *Intelligenza artificiale tra etica e diritti*, 2020, (p. 537)

tratta di una possibilità quanto più concreta se si considera l'elevata probabilità di ottenere identificazioni false.
In aggiunta, la diffusa prassi di utilizzo occulto da parte degli organi di polizia di tale tecnologia aumenta esponenzialmente la paura di un'applicazione non integralmente rispettosa dei diritti fondamentali degli individui.
La sostanziale assenza di una base normativa idonea a fornire al trattamento un fondamento di liceità comporta un impiego eccessivamente disinvolto dell'intelligenza artificiale negli ambiti più disparati. Inoltre, la mancata regolamentazione di tali strumenti si riverbera negativamente anche sul piano più strettamente processuale, rendendo dubbia l'utilizzabilità nel procedimento penale degli elementi raccolti mediante l'impiego di questi *software*.

A fronte delle problematiche finora emerse le prospettive future di una tale strumentazione sono potenzialmente due.
Sotto un primo profilo, è possibile ipotizzare uno scenario in cui venga proibito l'utilizzo delle tecnologie *de quo*. In questo modo, però, le forze dell'ordine si priverebbero di una tecnologia formidabile per la prevenzione e repressione dei reati.
Sotto un secondo profilo, l'ipotesi più auspicabile, seppur certamente più impegnativa, parrebbe quella di adeguarsi alla realtà, sfruttando le potenzialità offerte da questi sistemi ed elaborando al contempo una regolamentazione capace di limitarne quanto più possibile gli abusi.
Occorre, quindi, una disciplina totalmente nuova e "costituzionalmente orientata"[198] in grado di assicurare il rispetto della dignità, della libertà, e dell'eguaglianza[199].
Si tratta di un percorso che richiederà però un contributo anche alla comunità scientifica. La sfida si articolerà anche sul piano etico nello sviluppo di sistemi di intelligenza artificiale in grado di porre l'individuo al centro del processo e pertanto in grado di salvaguardarne gli interessi. Il legislatore, dal canto suo, sarà chiamato ad elaborare una soluzione in grado di diffondere tra i cittadini la fiducia verso un progresso di tale portata.

---

[198] C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo*, Rivista trimestrale Speciale, 2019, (p. 102 ss)
[199] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in *Ricerche giuridiche* n. 224, 2021, (p. 350 ss)

In tal modo le tecnologie di riconoscimento non verranno considerate quali manifestazioni odiose di un potere al quale è necessario sottomettersi[200], ma come strumenti al servizio dell'essere umano.

[200] *Ibidem*

Bibliografia

Ada Lovelace Institute. (2019). *Beyond face value: public attitudes to facial recognition technology*. Nuffield Foundation. 1-28. https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf

BALDACCINI, A. (2008). Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases. *European Journal of Migration and Law*, *10*(1), 31-49. https://doi.org/10.1163/138836407X261308

BALOSSINO, N., & SIRACUSA, S. (2004). *Security Forum 2004*. ItaSForum. 171–188.

BARILE, P. (1984). Diritti dell'uomo e libertà fondamentali. Il Mulino.

BORGIA, G. (2021). Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario. *La legislazione penale*, (4/2021), 206–226. https://www.lalegislazionepenale.eu/wp-content/uploads/2022/03/Fasc-4_2021.pdf

CASONATO, C. (2019). Intelligenza artificiale e diritto costituzionale: prime considerazioni. *Diritto pubblico comparato ed europeo, Rivista trimestrale*, (Speciale/2019), 101–130. https://www.rivisteweb.it/doi/10.17394/93043

CNIPA, C. N. p. l. n. P. A. (2004). *Linee guida per le tecnologie biometriche* (Gruppo di lavoro per le tecnologie biometriche). 1-140. https://www.ordineavvocatitrani.it/wp-content/uploads/2021/01/linee_guida_tecnologie_biometriche.pdf

Comitato Nazionale per la Bioetica. (2010). *L'identificazione del corpo umano: profili bioetici della biometria* (Parere del CNB). 1-22. https://bioetica.governo.it/media/1846/p95_2010_identificazione-corpo-umano-biometria_it.pdf

CURRAO, E. (2021). Il riconoscimento facciale e i diritti fondamentali: quale equilibrio? *Diritto penale e uomo*, (5/2021), 68–92. https://dirittopenaleuomo.org/wp-content/uploads/2021/05/DPU-5-2021.pdf

DELLA TORRE, J. (2020). Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice. *Diritto penale contemporaneo - Rivista Trimestrale*, (1/2020), 231–247. https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_1_2020_Della%20torre.pdf

DELLA TORRE, J. (2022). Quale spazio per i tools di riconoscimento facciale nella giustizia penale? In Di Paolo, G. & Pressaco, L. (A cura di), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio. Vol. 63. Editoriale Scientifica, Collana Quaderni della Facoltà di Giurisprudenza*. Università degli Studi di Trento. 7-61. https://iris.unitn.it/retrieve/handle/11572/361122/598564/IAiris20.12.22.pdf

European Union Agency for Foundamental Rights, F. (2015). *Smart Borders Pilot Project Technical Report Annexes Volume 2* (Report). https://home-affairs.ec.europa.eu/system/files/2020-09/smart_borders_pilot_-_technical_report_annexes_en.pdf

European Union Agency for Fundamental Rights, F. (2018). *Under watchful eyes: biometrics, EU IT systems and fundamental rights*. 1–135. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf

European Union Agency for Fundamental Rights, F. (2020). *Facial recognition technology: fundamental rights considerations in the context of law enforcement*. 1-36. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

FANUELE, C. (2009). *Dati genetici e procedimento penale*. CEDAM.

FIANDACA, G., & DI CHIARA, G. (2003). L'imputato e il diritto di difesa: il telaio dell'art. 24 Cost. E il "nuovo" catalogo dei diritti dell'«accusato». In *Una introduzione al sistema penale. Per una lettura costituzionalmente orientata* (pp. 368). Jovene.

FLORIDI, L. (2017). *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*. Raffaello Cortina Editore.

Garante per la Protezione dei Dati Personali, GDPD. *Provvedimento n. 440 del 26 Luglio 2018*. 26 Luglio 2018, www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9040256

Garante per la Protezione dei Dati, GDPD. *Provvedimento n. 127 del 25 Marzo 2021*. 25 Marzo 2021, www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877

GARLATI, L. (2021). Alle origini della prova scientifica: la scuola di polizia di Salvatore Ottolenghi. *Revista Brasileira de Direito Processual Penal*, *7*(2), 883–934. https://doi.org/10.22197/rbdpp.v7i2.597

GAROFOLI, F. I. (2020). Il rischio inquisitorio negli strumenti di intelligenza artificiale. (Cacucci Editore, Ed.). *Intelligenza Artificiale Tra Etica e Diritti Prime Riflessioni a Seguito Del Libro Bianco Dell'Unione Europea*, 537–574.

GRECO, L., & MANTELERO, A. (2018). Industria 4.0, robotica e privacy-by-design. *Il diritto dell'informazione e dell'informatica*, (6/2018), 875–900.
Gruppo di lavoro Articolo 29 per la protezione dei dati. (2012). *Parere 16/2011 relativo al riconoscimento facciale nell'ambito dei servizi online e mobili* (00727/12/IT WP 192). https://www.garanteprivacy.it/documents/10160/2150354/wp192

High Court of Justice, Queen's Bench Division, Divisional Court, 4 settembre 2019, Case No: CO/4085/2018, R (Bridges) v. CCSWP e SSHD

VAN DER PLOEG, I. (2005) *Biometric identification technologies: ethical implications of the informatization of the body*. Biometric Technology & Ethics, BITE Policy Paper no.1.

LIN, L., & MILHAUPT, C. (2023). *China's Corporate Social Credit System: The Dawn of Surveillance State Capitalism? The China Quarterly*, 1-19. doi:10.1017/S030574102300067X https://www.cambridge.org/core/journals/china-quarterly/article/chinas-corporate-social-credit-system-the-dawn-of-surveillance-state-capitalism/EC80AC0CC9AE60D3D3C631A707A5CE54

MASINI, E. (2022). *Sacro arsenale ovvero Pratica dell'Officio della Santa Inquisizione*. Anguana Edizioni.

Ministero dell'Interno Dipartimento della 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*.

MOBILIO, G. (2021). *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative: Vol. 224. Ricerche giuridiche*. Editoriale Scientifica.

PINO, G. (2006). *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali*. In *Libera circolazione e protezione dei dati personali* (p. 257–321). Giuffrè.

SACCHETTO, E. (2019). Spunti per una riflessione sul rapporto fra biometria e processo penale. *Diritto penale contemporaneo - Rivista Trimestrale*, (2/2019), 468–480. https://dpc-rivista trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019.pdf

SACCHETTO, E. (2020). Face to face: il complesso rapporto tra automated facial recognition technology e processo penale. *La legislazione penale*, 1–14. https://iris.unito.it/retrieve/e27ce430-df65-2581-e053-d805fe0acbaa/Sacchetto-finale.pdf

SAPONARO, L. (2022). Le nuove frontiere dell'individuazione personale. *Archivio Penale*, (1), 20. https://archiviopenale.it/File/DownloadArticolo?codice=d6883091-5b6e-4d31-b6d0-c8a40cf787de&idarticolo=33267

SARRA, C. (2022). *Il mondo-dato. Saggi su datificazione e diritto* (2nd ed., Ser. Scienze giuridiche). Cleup.
VASSALLI, G. (1957). *Il diritto alla libertà morale: contributo alla teoria dei diritti della personalità*. Utet.

Sitografia

TRECCANI (n.d) *Biometria*. Data dell'ultima consultazione: 12/06/2023, da https://www.treccani.it/enciclopedia/biometria

TRECCANI (n.d) *Repere*. Data dell'ultima consultazione: 20/06/2023, da https://www.treccani.it/vocabolario/ricerca/repere/

SWGDE (2023) *Glossary*. *Digital Evidence.* Data dell'ultima consultazione: 01/07/2023, da https://www.swgde.org/glossary

GARVIE, C. (2019) *Garbage in, Garbage out. Face recognition in flawed data*. Data dell'ultima consultazione: 18/07/2023, da https://www.flawedfacedata.com/

VALERI, M. (2022) *Mettiamoci la faccia*. Data dell'ultima consultazione: 22/07/2023, da https://poliziamoderna.poliziadistato.it/articolo/3536228dc7e38a89165859531

LAMORGESE, L. (2021) *Resoconto stenografico dell'Assemblea. Seduta n. 463 di mercoledì 3 marzo 2021*. Data dell'ultima consultazione: 24/07/2023, da https://www.camera.it/leg18/410?idSeduta=0463&tipo=stenografico

ANGIUS, R., & COLUCCINI, R. (a cura di) (2019) *Riconoscimento facciale, nel database di Sari quasi 8 schedati su 10 sono stranieri.* Data dell'ultima consultazione: 23/09/2023, da https://www.wired.it/attualita/tech/2019/04/03/sari-riconoscimento-facciale-stranieri/

GUZZONATO, C. (a cura di) (2022) *Che cos'è e come funziona il sistema di credito sociale in Cina*. Data dell'ultima consultazione: 10/08/2023, da https://www.focus.it/tecnologia/digital-life/cos-e-e-come-funziona-il-sistema-di-credito-sociale-cinese