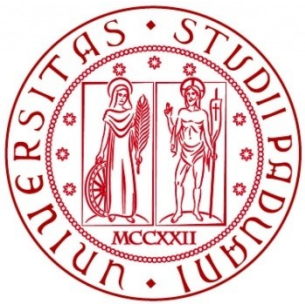

UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Diritto pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

Tesi di laurea

Sistemi di riconoscimento facciale: luci e ombre

Relatore:

Prof.re Massimo Bolognari

Laureando:

Nicolò Bergamin

[Matr. 2052118]

Anno Accademico 2023\2024

Indice

INTRODUZIONE

L'innovazione tecnologica dell'ultimo ventennio ha apportato delle novità sostanziali in tutti gli aspetti della vita degli individui, parimenti anche il perimetro giuridico e la cornice regolatoria del diritto penale in particolare ne sono stati travolti.

L'intelligenza artificiale ha modificato alcuni aspetti delle fasi investigative e di mantenimento della pubblica sicurezza, introducendo nuovi strumenti, come gli algoritmi predittivi e i sistemi di riconoscimento facciale utili al fine identificativo e di controllo di determinate aree sensibili.

L'elaborato verte su un'analisi di suddette tecnologie, con particolare riguardo alle tecnologie di riconoscimento facciale, tra cui l'applicativo SARI e le conseguenti pronunce del Garante per la protezione dei dati personali, il quale ha valutato tale tecnologia sotto il profilo della protezione dei dati personali e nel rispetto dei diritti fondamentali alla luce del quadro normativo nazionale e sovranazionale.

Tale tesi vuol dare una prospettiva circa i possibili aspetti positivi e le criticità che sorgono dall'impiego di queste tecnologie, anche sulla base degli ultimi sviluppi normativi fatti nell'eurozona, come il Regolamento 2024/1689 EU più comunemente noto con il nome di *AI Act.*

CAPITOLO I

1. L'intelligenza artificiale e gli strumenti predittivi nel processo penale

L'intelligenza artificiale (IA) viene definita come quella famiglia di tecnologie in grado di riprodurre alcune delle capacità cognitive dell'uomo (ragionamento, apprendimento, pianificazione e creatività)[1] , caratterizzata dall'utilizzo di grandi quantità di dati, un'elevata capacità computazionale e l'impiego di algoritmi. I ricercatori di IA enfatizzano un concetto di razionalità più che di intelligenza. Ciò dipende in primis dal problema definitorio di intelligenza, che non caratterizza solamente la «mente» meccanica ma anche quella umana: ««razionalità» si intende la capacità di scegliere la migliore azione da intraprendere per conseguire un determinato obiettivo alla luce di alcuni criteri di ottimizzazione delle risorse a disposizione»[2]. La tecnologia arriva alla scelta razionale analizzando e interpretando i dati, dando poi all'attuatore delle sue deduzioni (ovvero l'operatore umano), le coordinate verso cui muoversi:

[1] Che cos'è l'intelligenza artificiale? | Tematiche | Parlamento europeo (europa.eu)
[2] F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in Diritto Penale e Uomo, fascicolo 10/2019, 29 settembre 2019. P. 5

«il ragionamento o l'elaborazione delle informazioni è un processo operato attraverso un algoritmo che acquisisce come input i suddetti dati per poi proporre un'azione da intraprendere alla luce dell'obiettivo da raggiungere»[3].

L'IA si è trasformata nell'ultimo ventennio da mera ipotesi fantascientifica ad una realtà accessibile a tutti, o quasi, diventando un pilastro delle società contemporanee; tale nuova «istituzione» ha comportato delle novità sostanziali nelle vite delle persone[4].

In questo senso anche il campo giuridico ne è stato travolto: già da diversi anni vengono utilizzati strumenti basati sull'IA. Si pensi, ad esempio, agli strumenti che automatizzano determinate fasi del lavoro del giurista[5] (come i *software* per l'analisi di documenti legali) mentre nell'ambito del diritto penale in particolare vengono utilizzati a fini di giustizia predittiva, per il riconoscimento biometrico (c.d. strumenti o tecniche di riconoscimento facciale), ma anche in sede processuale per diminuire l'asimmetria informativa tra accusa e difesa[6].

---

[3] F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in Diritto Penale e Uomo, fascicolo 10/2019, 29 settembre 2019. P. 6

[4] Parafrasando J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, (a cura di) Ilaria MIcheli , in: Ragioni Comuni 2019 – 2020, P. 168

[5] DeepL, *Cinque strumenti di intelligenza artificiale che stanno rivoluzionando gli studi legali*, 14 novembre 2023

[6] R. E. KOSTORIS, *Intelligenza artificiale, strumenti predittivi e processo penale*, in www.discrimen.it, 5 marzo 2024. P. 4

I penalisti più progressisti[7] da tempo sostengono come l'utilizzo di questi *tools,* si pensi all'impiego di algoritmi predittivi per anticipare dove potrebbe realizzarsi un determinato reato, preidentificarne il soggetto autore ed in alcuni casi valutarne come conseguenza la pericolosità sociale[8], possano rappresentare uno strumento amico delle forze di *law enforcemet,* agevolando il mantenimento della pubblica sicurezza e la prevenzione dei reati[9].

L'algoritmo è la «specificazione di una sequenza finita di operazioni elementari, eseguibili facilmente da un elaboratore che, a partire da un insieme di dati I (input), produce un altro insieme di dati O (output) che soddisfano un preassegnato insieme di requisiti»[10]. L'algoritmo predittivo è quindi un'espressione matematica che permette di risolvere o, meglio, nel nostro caso di aiutare l'agente nel condurre determinate operazioni, siano esse di analisi, controllo o decisorie.

[7] In merito si vedano le posizioni in materia di J. DELLA TORRE, F. BASILE e G. LASAGNI

[8] poiché solitamente l'analisi si basa su soggetti già identificati, v. G. LASAGNI, *Difendersi dall'intelligenza artificiale o difendersi con l'intelligenza artificiale? Verso un cambio di paradigma,* Intelligenza artificiale e processo penale – indagini prove e giudizio, (a cura di) Gabriella Di Paolo e Luca Presacco, P. 63-84

[9] Una simile considerazione si può leggere nel *paper* del convegno di esperti di polizia del 2019 in materia di IA e *law enforcement* organizzato dall'OSCE nel 2019. *Annual Police Experts Meeting: Artificial Intelligence and Law Enforcement: An Ally or an Adversary?,* 23-24 September, in, rivista Redazione,: «Anche se l'uso dell'IA nel lavoro delle forze dell'ordine è un argomento relativamente nuovo, alcuni strumenti basati sull'intelligenza artificiale sono già stati testati e sono persino attivamente utilizzati dai servizi di polizia di diversi Paesi del mondo. Questi includono software di analisi di video e immagini, sistemi di riconoscimento facciale, di identificazione biometrica, droni autonomi e altri robot e strumenti di analisi predittiva per prevedere le "zone calde" del crimine»

[10] Definizione in ambito informatico: Algoritmo, Enciclopedia Treccani, www.treccani.it

Tali *tool* matematici sono, inoltre, parte integrante di tutti quei sistemi che svolgono attività di contrasto, in uso alle forze di polizia e magistratura; tali strumenti, capaci di leggere la biometrica dei soggetti, vengono denominati «tecnologie o tecniche di riconoscimento facciale», riferendosi così, a quegli applicativi, che, sulla base di specifici dati e algoritmi sono in grado di «automatizzare le procedure di verifica dell'identità, attraverso la valutazione di caratteristiche fisiologiche della persona»[11]

La mole di strumenti basati sull'IA e sugli algoritmi è quindi notevole in campo penale, da dispositivi di ricerca e di accesso dei dati, a quelli per efficientare la giustizia[12].

Va tuttavia, sottolineato come, il fine predittivo nel diritto penale è un concetto che assume un significato probabilistico, si tratta della possibilità di effettuare stime e previsioni basandosi su dati storici: «Predizione è infatti, una traduzione letterale della voce inglese *predictive*, ed è comunque un termine che viene impiegato con un particolare significato nelle scienze dure; trasponendolo in un ambito tipicamente umano, come quello della giustizia, esso finisce per non corrispondere al senso che la

[11] GIULIA LASAGNI, *Difendersi dall'intelligenza artificiale o difendersi con l'intelligenza artificiale? Verso un cambio di paradigma*, Intelligenza artificiale e processo penale – indagini prove e giudizio, (a cura di) GABRIELLA DI PAOLO e LUCA PRESACCO, Pag. 63-84

[12] ROBERTO E. KOSTORIS, *Intelligenza artificiale, strumenti predittivi e processo penale*, www.discrimen.it, 5 marzo 2024, Pag. 3

parola predizione assume nella lingua italiana in rapporto all'agire degli uomini, dove evoca l'idea del vaticinio, del preannuncio oracolare di eventi futuri; un'idea che, come è evidente, sta fuori del mondo del diritto, che è del tutto incompatibile con esso»[13] In ambito penale, tali strumenti possono essere utilizzati, ad esempio, per prevedere l'accadimento di un reato, fornendo l'eventuale percentuale di rischio di realizzazione dello stesso in un determinato ambiente socio-geografico di riferimento. Si allude agli strumenti c.d. di *predictive policing*[14], i quali dovrebbero permettere di effettuare un'analisi preventiva dei reati dettagliata: «la predizione si basa fondamentalmente su una rielaborazione attuariale di diversi tipi di dati, tra cui quelli relativi a notizie di reati precedentemente commessi, agli spostamenti e alle attività di soggetti sospettati, ai luoghi, teatro di ricorrenti azioni criminali, e alle caratteristiche di questi luoghi, al periodo dell'anno o alle condizioni atmosferiche maggiormente connesse alla commissione di determinati reati»[15]. Tali software hanno dato la possibilità di incrementare esponenzialmente l'accuratezza delle

[13] R. E. KOSTORIS, Intelligenza *artificiale, strumenti predittivi e processo penale*, in www.discrimen.it, 5 marzo 2024. P. 4

[14] J. DELLA TORRE, *quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in Intelligenza artificiale e processo penale – indagini prove e giudizio, (a cura di) G. DI PAOLO e L. PRESACCO. P.10 e R. E. KOSTORIS, *Intelligenza artificiale, strumenti predittivi e processo penale*, in www.discrimen.it,, 5 marzo 2024. P. 4

[15] F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine,* in, Diritto Penale e Uomo, fascicolo 10/2019, 29 settembre 2019. P.10

indagini; miglioramento dovuto principalmente dal riconoscimento di connessioni che l'operatore umano difficilmente individua[16].

Possiamo dividere gli strumenti predittivi assistiti dall'IA in due categorie:

A) Gli strumenti in grado di individuare i c.d. «*hotspot*», ovvero le «zone calde» e quindi gli scenari dove potrebbero avvenire le eventuali azioni criminose.

B) Gli strumenti basati sul «*crime linking*»[17], ossia quelli che seguono in modo accurato le attività di determinati soggetti.

Tuttavia, sorgono alcune problematiche in relazione a tali strumenti. In primo luogo, si corre il rischio di far «autoavverare» determinati output dati dall'algoritmo. Difatti, è logico presupporre, che più la ricerca dei reati sia massiccia in una determinata area (*hotspot*) o nei confronti di una determinata fascia di popolazione, maggiore sarà la probabilità che si venga a conoscenza di un numero crescente di reati, correndo il rischio di entrare quindi in un *loop* di intensificazione dei controlli in quella «zona calda». Allo stesso modo presenta un profilo problematico anche la profilazione degli individui, i quali potrebbero subire discriminazioni sulla

[16] C. CATH, S. WACHTER, B. MITTELSTADT, M. TADDEO, L. FLORIDI, Artificial Intelligence and the "Good Society": the US, EU, and UK approach, in Science and Eng. Ethics, 2018, pp. 505 ss.; L. BENNET MOSES, J. CHAN, Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability, in Policing and Society, 2016, pp. 1 ss.; G. Mastrobuoni, Crime is Terribly Revealing: Informationt Technology and Police Productivity, 2017

[17] ovvero un'analisi finalizzata all'identificazione di schemi comuni presenti nei crimini violenti questo al fine di collegare i delitti commessi dallo stesso soggetto anche se consumati in tempi e luoghi differenti

base di dati [18]erroneamente implementati da cui l'algoritmo trae le informazioni e sui quali questo viene allenato: «si evidenzia il rischio di c.d. *implicit bias*: da una parte laddove l'input non è completamente neutro, l'output dell'interrogazione rischia di essere influenzato da un pregiudizio, che può portare alla discriminazione di singoli individui o di gruppi sociali; dall'altra, l'algoritmo che è concepito e interpretato da un umano può[19]»[20].

Tali strumenti possono essere utilizzati anche per calcolare la probabilità di recidiva di un soggetto già condannato (c.d. *risk assesment tools*[21]); strumento che in questo caso aiuta il giudice in sede di commisurazione della pena[22]. A questo proposito va sottolineato come tali strumenti possano esternare un output viziato da *bias*[23] volontari o involontari implementati nell'algoritmo[24]. Proprio per questo, il giudice non

[18] Si allude alla pratica informatica per cui gli algoritmi a servizio di tecnologie basate sull'IA, vengono spesso allenati sulla base di grandi quantità di dati, se questi dovessero essere incompresi dalla macchina, l'output di conseguenza sarebbe difettoso.

[20] A. M. MAUGERI, *L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based practices e tutela dei diritti fondamentali*, in archivio penale 2021, n.1. P. 12

[21] R. E. KOSTORIS, *Predizione decisoria, diversion processuale e archiviazione,* editore Associazione "Progetto giustizia penale*"* c\o Università degli studi di Milano, Dipartimento di Scienze Giuridiche. P. 2

[22] Ibidem

[23] un risultato distorto, derivante da un errore nella progettazione o implementazione

[24] A tal proposito il caso statunitense Loomis vs. *Supreme Court of Wisconsis,* nel quale, il ricorrente lamentava una violazione del giusto processo, che non venne riconosciuta da parte della corte. Si evinse, tuttavia, come, l'algoritmo *Correctional Offender Management Profiling for Alternative Sanction* (COMPAS) utilizzato in sede di commisurazione della pena e protetto da segreto industriale, ragion per cui il suo funzionamento rimase sconosciuto, calcolasse sulla base di precedenti giudiziari e sulle risposte date ad un questionario la pena da commisurare e la probabilità di recidiva dell'imputato, che veniva aumentata del doppio per i soggetti afroamericani rispetto ai caucasici.

dev'essere vincolato dal risultato dato dalla macchina e non deve riporre una fiducia incontrovertibile nello strumento a sua disposizione, soprattutto per evitare una deresponsabilizzazione della sua figura e, in secondo luogo, per la mancanza di effettivo raziocinio della tecnologia in sé.

Sarebbe utile in questo caso promuovere una progettazione e sviluppo trasversale dell'algoritmo tra il produttore\sviluppatore del sistema a base di IA e il giurista, per evitare di commercializzare un sistema dannoso per gli individui sul piano dei diritti fondamentali e delle garanzie[25]. Deve altresì essere garantita all'individuo la possibilità di esercitare il diritto a «non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato in grado di incidere significativamente sulla sua persona», come traspone dal *General Data Protection Regulation* [26]; allo stesso modo, all'interno dei confini italiani ci si muove verso questa direzione. Il Consiglio di Stato ha messo in rilievo come «deve comunque esistere nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatica»[27]. Va però evidenziato come, in alcuni casi «le capacità umane di rivedere decisioni

[25] Come consigliato anche dalla Carta Etica, appendice I paragrafo 9- *"Potenzialità e limiti degli strumenti di giustizia predittiva"*, Pag. 39
[26] Art. 22 GDPR Regolamento 2016\679 UE e Art. 11 Direttiva 2016\680 UE
[27] Cons. St., sez. VI, sent. 4 febbraio 2020 n. 881, § 11.2

automatizzate siano tutto sommato limitate [...] a garantire un rimedio effettivo a chi subisce le conseguenze di una decisone automatizzata»[28] .

Altri strumenti utili ai fini investigativi che utilizzano algoritmi predittivi sono, come velocemente accennato in precedenza, gli strumenti in grado di riconoscere un volto presente in un'immagine o in un flusso video attraverso l'analisi di dati biometrici. Si tratta di strumenti c.d. «misti»: «perché, pur mirando alla conoscenza di dati del presente[...]si fondano su un procedimento di inferenza per certi aspetti simile a quello degli strumenti predittivi, dato che prendono a parametro dell'algoritmo elementi noti o conoscibili del passato[29].

Va, infine, messa in rilievo la mancanza di trasparenza che caratterizza troppo spesso questi algoritmi, essendo questi il più delle volte protetti dal diritto d'autore e segreto industriale, con la conseguenza di non riuscire ad avere abbastanza informazioni sul loro funzionamento e sui parametri utilizzati. Diviene quindi ragionevole auspicare un intervento legislativo, al fine di rendere conoscibili gli elementi non acquisibili che costituiscono l'algoritmo, per evitare di rendere i principi processuali incerti. [30]

---

[28] G. LASAGNI, *Difendersi dall'intelligenza artificiale o difendersi con l'intelligenza artificiale? Verso un cambio di paradigma*, Intelligenza artificiale e processo penale – indagini prove e giudizio, (a cura di) G. DI PAOLO e L. PRESACCO. P. 70

[29] R. E. KOSTORIS, *Intelligenza artificiale, strumenti predittivi e processo penale* , in www.discrimen.it, 5 marzo 2024. P. 6.

[30] A. M. MAUGERI, *L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based pratices e tutela dei diritti fondamentali,, in* archivio penale 2021, n.1. P. 19

Queste prime considerazioni portano inevitabilmente ad una riflessione, in relazione ai dati di cui questi strumenti si nutrono, ovvero i c.d. dati biometrici.

2. Il dato biometrico

«Usando una immagine, si potrebbe sostenere che i dati biometrici rappresentino una forma di digitalizzazione del corpo umano»[31]

Con il termine dato biometrico ci riferiamo a «dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»[32] . In tale categoria rientrano, quindi, le impronte facciali o digitali, la forma della mano, dell'iride, il timbro della voce, la firma e l'andatura[33]. Il dato in questione viene analizzato attraverso operazioni matematiche e viene «collegato» ad un preciso soggetto grazie alle peculiarità individualizzanti di ogni essere umano.

[31] G. MOBILIO, *Tecnologie di riconoscimento facciale*, Editoriale scientifica, 2021, Ricerche giuridiche collana diretta da A. CELOTTO, F. LIGUORI, L. ZOPPOLI, P. 136.
[32] regolamento europeo (GDPR) all'art. 4, par. 1, n. 14
[33] J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, in: (a cura di) Ilaria MIcheli , in Ragioni Comuni 2019 – 2020.

Tali dati hanno le caratteristiche dell'esclusività in quanto individualizzanti, dell'idoneità a identificare l'individuo[34], della permanenza, in quanto rimangono pressoché inalterati durante tutto il corso della vita e della collezionabilità in quanto i dai possono essere collezionati e ri-utilizzati più volte[35].

«Il dato biometrico è quindi una specie di "codice a barre" che rende possibile distinguere un soggetto da un altro e allo stesso modo lo rende identificabile»[36]. Tale dato rientra nella categoria dei c.d. dati a trattamento speciale[37], che ricevono una tutela rafforzata da parte del legislatore europeo, nel momento in cui attraverso il trattamento di questi si può giungere all'identificazione univoca o all'autenticazione di una persona fisica; per il trattamento di questa categoria di dati è necessario che sussista una base giuridica[38] di cui al comma 2 art. 9 Reg. 679\2016 (GDPR), la quale può essere rappresentata, ad esempio, dal consenso esplicito dell'interessato per il trattamento di dati personali con finalità specifiche, quando il trattamento di questa categoria di dati è necessario

[34] *Dati biometrici cosa sono e come vengono utilizzati*, in www.profiler.cloud

[35] G. MOBILIO, *"Tecnologie di riconoscimento facciale"*, Editoriale scientifica, 2021, Ricerche giuridiche collana diretta da A. CELOTTO, F. LIGUORI, L. ZOPPOLI, pag. 137

[36] Ibidem

[37] Ex. art. 9 GDPR regolamento EU 2016\679. "1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona."

[38] Su cui si fondi il trattamento di dati in esame, il quale deve rispettare, vari principi, liceità, correttezza e trasparenza

per tutelare un interesse vitale dell'interessato, quando i dati sono resi personalmente pubblici dall'interessato e quando il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ancora ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni, detto ciò, va sottolineato come tali informazioni siano considerate dal GDPR come dati particolarmente personali e sensibili; in ragione di ciò: «bisogna tenere in considerazione il caso concreto e valutare se sussistono alternative al trattamento nella stessa misura efficaci e meno invasive»[39], rispetto al trattamento di questa categoria di dati. In tema di riconoscimento facciale bisogna fare riferimento al considerando 51 del *General Data Protection Regulation* (GDPR), il quale prevede che: «Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico (hardware o software) che consente l'identificazione univoca o l'autenticazione di una persona fisica[40]. In caso contrario sono tutelati come normali dati personali. Da questo possiamo dedurre che, solamente nel caso in cui il fine sia quello identificativo il dato potrà essere considerato come dato biometrico;

[39] S. GIRARDI, *Dati biometrici. Quo vadis per un trattamento legittimo?,* 23 Aprile 2021, in Dati biometrici. Quo vadis per un trattamento legittimo? (altalex.com)
[40] Dati biometrici - Protezione dati personali

concetto ribadito anche dal Garante della privacy italiano[41] il quale ha sottolineato come si rientri nell'alveo dei dati biometrici solamente quando si utilizzano algoritmi di *facial recognition* i quali conservano il «*template»,* a differenza degli algoritmi *face detection,* i quali non conservano l'elaborato algoritmico[42]senza identificarlo[43].

Tutti gli elementi di cui si è discusso fino a questo punto (IA, algoritmi, strumenti predittivi e dati biometrici), ci portano al nocciolo dell'argomento su cui verte suddetta tesi, ovvero i sistemi di riconoscimento facciale.

3. I sistemi di riconoscimento facciale

I sistemi o software di riconoscimento facciale sono un gruppo eterogeneo di *tools* che permettono l'automatizzazione di alcune procedure di verifica dell'identità rendendo autonome le fasi di analisi delle caratteristiche fisiologiche, essi vengono definiti come: «applicativi che permettono di

[41] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, "*Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferro- viaria, 21 dicembre 2017, con cui il Garante ha consentito la prosecuzione del tratta- mento dei dati da parte di un sistema di tipo "digital signage", che tramite una web- cam si limita a effettuare la raccolta di dati audience per personalizzare l'offerta pubblicitaria e realizzare analisi di tipo statistico, operano una raccolta di dati a partire da tecniche di "face detection" che valutano l'età, il sesso, la risposta emozionale dello spettatore"*

[43] V. LA VECCHIA, Caratteristiche e differenza tra Face Detection e Face Recognition, Informatica e Ingegneria Online, in vitolavecchia.altervista.org

analizzare in modo automatico immagini digitali contenenti volti di individui per scopi di identificazione, autenticazione\verifica, o categorizzazione di suddetti individui»[44].

Le tecnologie di riconoscimento facciale si fondano principalmente su due applicativi, che, utilizzati in modalità combinata costituiscono la c.d. tecnologia di facial *recognition*[45]: il primo elemento costitutivo è la *face detection*[46]*,* in grado di riconoscere la presenza di un volto umano in un flusso video o in un'immagine statica, ma non in grado di identificarlo, rilevando quindi la mera presenza umana. Si tratta di uno strumento che presenta delle potenzialità minori, ma non banali, in quanto delinea il primo passo verso l'obbiettivo identificativo;

Troviamo poi l'elemento di *facial recognition,* tecnologia capace di accertare, oltre alla presenza di un individuo (grazie alla presenza della *face detection)*, anche l'identità del soggetto e raffrontarla[47]. Difatti, viene in genere utilizzata a scopo identificativo; l'algoritmo si serve dei tratti individualizzanti di ciascun individuo che analizza per effettuare il confronto ed erogare l'output[48].

---

[44] J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, (a cura di) Ilaria MIcheli, in "Ragioni Comuni 2019 – 2020. P.169

[45] I quali però possono anche essere utilizzati separatamente

[46] Applicazione integrata nei sistemi di *facial recognition*

[47] il confronto avviene attraverso l'immagine ricevuta e quelle presenti nelle banche dati

[48]V. LA VECCHIA, Caratteristiche e differenza tra Face Detection e Face Recognition, Informatica e Ingegneria Online, in vitolavecchia.altervista.org

La tecnologia riconoscimento facciale[49] opera secondo una procedura standard[50]: come prima cosa recepisce «il dato grezzo» ovvero l'input rappresentato dall'immagine del volto dell'individuo, che verrà quindi analizzato, (questo può essere sia statico che dinamico), dopodiché riesce ad individualizzare alcune caratteristiche del volto all'interno del *frame* che sta analizzando ed attraverso il c.d. *embedding* proietta in uno spazio vettoriale i caratteri biometrici analizzati, e ne traccia la posizione di occhi, naso e orecchie; infine, elabora attraverso delle operazioni matematiche, un modello, il c.d. *template*[51] il quale viene poi confrontato con delle immagini di individui presenti su banche dati e nel caso in cui risulti una possibilità che le due immagini si riferiscano alla stessa persona scatta il c.d. *matching*[52]. Tali strumenti, alimentati dai dati, in grado di tradurre immagini in informazioni binarie, vengono «allenati» a far ciò; uno dei prototipi fra i più diffusi, al fine di migliorare le capacità della tecnologia è sicuramente il modello c.d. *triplet loss:* «l'algoritmo riceve in input tre immagini, due della stessa persona e una di una terza; l'algoritmo aggiusta i suoi parametri in modo da massimizzare al

[49] Si intende il sopra citato *facial recognition,* composto anche dalla funzione di *face detection*
[50] Che però può essere sviluppata e implementata in modi differenti.
[51] Quando la tecnologia di *face detection* viene impiegata in modo autonomo, ossia, quando valuta la presenza o meno di un soggetto, all'interno di una video ripresa o di un'immagine, senza valutarne però l'identità, non conserva nessun *template*
[52] Parafrasando J. DELLA TORRE, *Algoritmi di facial recognition e procedimento penale italiano*, (a cura di) Ilaria MIcheli , in Ragioni Comuni 2019 – 2020. P. 169-170

contempo la similarità per le rappresentazioni delle prime due, e la differenza con la terza rappresentazione; il passaggio è ripetuto milioni di volte, su diverse triplette di immagini, così da garantire l'assimilazione di regole efficaci ma generiche»[53].

Le tecnologie di riconoscimento facciale hanno, come si può immaginare, suscitato euforia negli operatori di *law enforcement,* i quali sono stati dotati di applicativi dalle potenzialità notevoli in grado di «leggere» e tradurre le caratteristiche del volto umano.

Analizzando i benefici che derivano dall'impiego di tale tecnologia possiamo vedere come, in primo luogo, la rapidità di tali strumenti sia in grado di minimizzare i tempi ed il lavoro dell'operatore. Prima della concessione di tali strumenti era l'operatore umano che doveva manualmente inserire i dati e connotati del soggetto ricercato. In secondo luogo, tali tecnologie «prendono in considerazione una nutrita serie di criteri fisionomici e metrici, dotati di portata individualizzante, essendo persino in grado di estrarre caratteristiche fisionomiche non percepibili dall'occhio umano»[54].

[53] L. BAIOCCO, E. FERRI, L. R. CELSI, *Riconoscimento facciale automatico: opportunità e minacce*, 22 febbraio 2021, in www.ai4business.it

[54] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in INTELLIGENZA ARTIFICIALE E PROCESSO PENALE: INDAGINI; PROVE E GIUDIZIO; a cura di G. Di Paolo, L. Presacco, Pag. 15.

Altro aspetto positivo degno di nota, riguarda la ripetibilità dell'analisi dei volti da parte degli strumenti di riconoscimento facciale, cosa che invece non si può dire per il riconoscimento di soggetti da parte di un operatore umano, il quale è soggetto «all'inevitabile degradazione mnestica tipica della mente umana»[55]: l'identificazione di un soggetto è un'attività cognitiva legata al ricordo delle generalità fisiche dell'individuo che si cerca di identificare o riconoscere, proprio per questo, si tratta di una attività psicologicamente irripetibile[56], dovuta anche da una diminuzione dei ricordi nel tempo; la macchina salvo perdita di dati è in grado di anatomizzare l'immagine di un volto un numero indeterminato di volte[57]. Sono dunque strumenti che possono prestarsi ad una molteplicità di usi: possono essere dispiegati sia per quanto riguarda l'identificazione di un soggetto (si pensi ad una scena del crimine, l'identificazione del soggetto è utile «sia per orientare le indagini sia in chiave probatoria»[58]), ma anche come strumento di controllo di determinate aree sensibili, ad esempio, aeroporti o luoghi dove avvengono manifestazioni, verificando la presenza di soggetti sospettati, indagati o vittime di reati.

[55] Ibidem
[56] Si pensi ad un soggetto visto una sola volta, l'identificazione di questo può risultare assai complessa.
[57] Parafrasando J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in INTELLIGENZA ARTIFICIALE E PROCESSO PENALE: INDAGINI; PROVE E GIUDIZIO; a cura di G. Di Paolo, L. Presacco, Pag. 15.
[58] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in INTELLIGENZA ARTIFICIALE E PROCESSO PENALE: INDAGINI; PROVE E GIUDIZIO; a cura di G. Di Paolo, L. Presacco, P. 16.

Ciò fin qui detto però, fa ben capire, come, tale tecnologia abbia anche degli aspetti critici; un primo aspetto negativo che caratterizza tali strumenti è l'incertezza dell'accuratezza del risultato prodotto in relazione ai falsi-positivi e falsi-negativi che il sistema produce; invero, come accennato in precedenza, il risultato ottenuto è un risultato probabilistico; il che significa che vi è sempre una percentuale di errore da parte dell'algoritmo, dovuto ad esempio alla risoluzione dell'immagine, alla luce, ai movimenti ripresi e analizzati, ma anche dalla pettinatura del soggetto o dal *make-up* utilizzato.

Per falso positivo facciamo riferimento a quella situazione in cui, la macchina erroneamente ritiene che vi sia un *match* tra l'immagine analizzata e l'immagine conservata in un data base. Al contrario, si verificherà un falso negativo qualora l'algoritmo non riconosca un *match* tra i due elementi analizzati, non facendo in questo modo scattare l'*alert,* e di conseguenza, ad esempio, non informando la polizia di frontiera, la quale potrebbe consentire il passaggio ad un valico di un soggetto ricercato.

Tuttavia, «attualmente sono stati sviluppati algoritmi altamente performanti e sofisticati che, con immagini di buona qualità, consentono di identificare un soggetto la cui immagine è acquisita in ambienti

controllati con un tasso di errore dello 0,1% nel confronto con gallerie di decine di milioni di immagini»[59].

Arrivati a questo punto e alla luce di quanto appena detto, si procederà con un'analisi più approfondita dei sistemi di riconoscimento faciale, di cui, alcuni in uso nel nostro paese.

[59] G. MOBILIO, Tecnologie di riconoscimento facciale, Rischi per i diritti fondamentali, e sfide regolative, in Ricerche giuridiche n. 224, 2021, Pag. 36-37

CAPITOLO II

1. I sistemi di riconoscimento facciale in Italia

Accanto agli strumenti tipici in materia di ricognizione (art. 213 c.p.p.) e individuazione (art. 361 c.p.p.), troviamo le tecnologie di riconoscimento facciale. Questo accostamento è la conseguenza della loro importante e rapida diffusione e delle loro notevoli potenzialità.

In Italia, si è cercato di dare a suddette tecnologie uno spazio all'interno del procedimento penale, anche se indebitamente, in relazione all'assenza di un preliminare intervento legislativo: le tecnologie di riconoscimento facciale non sono mai state regolate in Italia con un intervento legislativo su misura, l'impiego di questi applicativi da parte delle autorità risulta atipico in quanto non disciplinate dalla legge.

A tal proposito, su iniziativa del Ministero degli interni, nel 2017, fu avviata una procedura ad evidenza pubblica[60] con il fine di fornire alla

[60] strumento attraverso il quale la P.A. svolge la sua attività negoziale, nell'individuazione di un contraente per il reperimento sul libero mercato di forniture, servizi e opere.

polizia giudiziaria[61] un'infrastruttura cibernetica denominata: "*Sistema Automatico di Riconoscimento delle Immagini-S.A.R.I.".*

Si tratta di uno strumento completamente *made in Italy* che incorpora la tecnologia di *facial recognition*: tale software è stato commissionato dalla Direzione Centrale Anticrimine ad una società privata Italiana[62]: le principali (e insoddisfacenti) informazioni che si possono rinvenire per quanto riguarda il funzionamento «interno» dell'applicativo sono costituite dal capitolato tecnico[63] allegato al contratto tra il Ministero e l'azienda commissionata. Le informazioni reperibili rivelano come il mandatario abbia richiesto lo sviluppo di un sistema in grado di riconoscere in modo autonomo e automatico i volti al fine identificativo, a partire da immagini statiche nella versione *Enterprise* o dai fotogrammi che compongono un video nella versione *Real-time*.[64] L'algoritmo è stato valutato in modo eccellente dal *NIST - National Institute of Standards and Technology*[65] , considerandolo come uno dei migliori al mondo ,

[61] In uso ai Carabinieri e alla Polizia di stato
[62] azienda Leccese denominata PARSEC 3.26.
[63] Ministero dell'Interno, Dipartimento di pubblica sicurezza, *Capitolato tecnico. Procedura volta alla formitura della soluzione integrata per il Sistema Automatico di Riconoscimento delle Immagini S.A.R.I.*, in www.poliziadistato.it, , 27 giugno 2016.
[64] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in INTELLIGENZA ARTIFICIALE E PROCESSO PENALE: INDAGINI; PROVE E GIUDIZIO; a cura di G. Di Paolo, L. Presacco, P. 31-32
[65] Ente statunitense che valuta gli algoritmi e le loro performance

l'applicativo è costantemente aggiornato e testato sul grande archivio[66] nella disponibilità delle forze di polizia.[67]

Tale sistema di riconoscimento facciale ha infatti già subito una ristrutturazione tra il 2020 ed il 2021: questo si è reso necessario in quanto, le tecnologie di riconoscimento facciale sono una famiglia di tecnologie neonate, che richiedono continui aggiornamenti e aggiustamenti: «Ne consegue che le iniziative volte a modernizzarli non possono che essere lette favorevolmente: solo in questo modo è possibile renderli davvero affidabili, riducendo il rischio di false individuazioni»[68].

Va sottolineato, tuttavia, come il processo decisionale di implementare tali strumenti sia stato poco trasparente in Italia, senza un effettivo dibattito pubblico: l'intervento più significativo al quale è stato dato maggior visibilità riguarda le due istruttorie avviate dal Garante della Privacy italiano in relazione alle implicazioni per la protezione dei dati dei soggetti coinvolti; a differenza di altri paesi come gli Stati Uniti; dove sono stati fatti importanti passi in materia di normazione per quanto concerne i

[66] Si fa riferimento alla piattaforma AFISS-SSA

[67] M. VALERI, *Mettiamoci la faccia*, 2022, in https://poliziamoderna.poliziadistato.it/articolo3536228dc7e38a89165859531

[68] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in INTELLIGENZA ARTIFICIALE E PROCESSO PENALE: INDAGINI; PROVE E GIUDIZIO; a cura di G. Di Paolo, L. Presacco, P.35

sistemi di riconoscimento facciale[69], o in Cina[70] e Russia le quali hanno sdoganato del tutto tali sistemi di controllo, con tutto quello che ovviamente ne comporta sul piano dei diritti per gli individui.[71]

4. S.A.R.I. Enterprise e il parere del Garante per la protezione dei dati personali

Nella modalità *Enterprise* S.A.R.I. dà la possibilità alle forze di polizia di individuare in tempistiche notevolmente brevi (circa quindici secondi) l'identità di un volto, presente in un'immagine già in possesso delle autorità, l'immagine è memorizzata in una banca dati, individuata nella piattaforma AFIS-SSA *Automated Fingerprint Identification System*[72]. Si tratta di banche dati preesistenti che sono state riprodotte all'interno del *cyber*-sistema S.A.R.I.: «ove confluiscono le immagini di diverse categorie di individui oggetto di fotosegnalazione (tra cui, ad esempio, indagati, oppure persone che non siano in grado di provare la loro identità,

[69] Ad esempio, l'approvazione della legge statale dello stato di Washington sull'uso delle tecnologie di riconoscimento facciale entrata in vigore nel 2021.

[70] Si vedano a tal proposito anche le nuove proposte presentate nel 2023 dalla *Cyberspace administration of China* finalizzate a garantire tutele più elevate per i cittadini ed i minori di 14 anni

[71] M. R. CARBONE, *SARI, il riconoscimento facciale nella pubblica sicurezza: servono regole e trasparenza* , 23 marzo 2021, in www.agendadigitale.eu

[72] Sistema di identificazione tramite impronte digitali

o, ancora, migranti) nonché le informazioni concernenti i loro dati anagrafici e biometrici»[73].

Secondo quanto detto nella risposta ad un'interrogazione parlamentare presentata al governo sul funzionamento di S.A.R.I., a inizio 2020 in AFIS-SSA erano presenti 17 milioni di cartellini fotosegnaletici corrispondenti a quasi 10 milioni di individui, di cui 2 milioni cittadini italiani[74].

Lo scenario *Enterprise* dà la possibilità di effettuare una verifica su più *layers*, a livello del volto, su base anagrafica e infine anche su base combinata di questi due elementi. Nel rispetto del capitolato tecnico, all'esaurirsi della verifica compiuta, l'algoritmo fornisce la c.d. *candidate list,* ossia una lista di soggetti, ordinati attraverso uno *score* il quale indica il grado di somiglianza tra il soggetto fotosegnalato e memorizzato nella banca dati e quello «ricercato»; dopodiché, viene richiesto l'intervento dell'operatore umano, il quale dovrà confermare o smentire il risultato algoritmico: «applicando le procedure di comparazione fisionomica,

[73] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in INTELLIGENZA ARTIFICIALE E PROCESSO PENALE: INDAGINI; PROVE E GIUDIZIO; a cura di G. Di Paolo, L. Presacco, P.33

[74] CECCANTI n.5-03482, in Atti Camera, I Commissione permanente, 5 febbraio 2020, in www.camera.it, pag. 61

rispetto alle quali le forze di polizia scientifica ricevono una specifica formazione[75].

Tale intervento umano è stato posto come presidio nel rispetto del c.d. principio *human in the loop-HITL: «*principio secondo cui gli esseri umani devono mantenere un ruolo attivo nel processo decisionale dell'intelligenza artificiale»[76] così facendo è possibile garantire il rispetto dei principi etici fondamentali in rapporto alle decisioni o previsioni algoritmiche.

Tuttavia, per quanto riguarda SARI *Enterprise,* il capitolato tecnico preannuncia la possibilità che questo si avvalga di algoritmi non testati dal *NIST*, con il conseguente rischio di abbassare il livello di sicurezza dell'applicativo in relazione all'esito della verifica compiuta e di conseguenza aumentare l'incertezza del risultato prodotto (il tasso di errore nelle individuazioni in questo scenario potrebbe aumentare) ma anche in relazione ad una limitazione delle garanzie, che di per sé sono già limitate, non essendo la collettività in grado di conoscere del tutto il funzionamento interno dell'applicativo.

[75] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in INTELLIGENZA ARTIFICIALE E PROCESSO PENALE: INDAGINI; PROVE E GIUDIZIO; a cura di G. Di Paolo, L. Presacco, P.33

[76] P. MARINONI, *Human in the Loop, l'uomo al centro dell'algoritmo*, 9 agosto 2023, in www.ainews.it

Come sopra citato, uno degli interventi più significativi in Italia per quanto riguarda S.A.R.I. è stato effettuato dal Garante per la protezione dei dati personali; tale autorità ha avviato due indagini con la finalità di valutare l'applicativo sotto la lente dei diritti fondamentali; la prima istruttoria conclusasi nel 2018 avente ad oggetto S.A.R.I. *Enterprise* ha escluso la «presenza di criticità sotto il profilo della protezione dei dati»[77] inoltre tale applicazione è rispettosa dell'art. 8 D.lgs.51/2018, il quale recita: «sono vietate le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge». A tal proposito il Garante ha sottolineato come: «Il trattamento in argomento costituisce, infatti, un mero ausilio all'agire umano, avente lo scopo di velocizzare l'identificazione, da parte dell'operatore di polizia, di un soggetto ricercato della cui immagine facciale si disponga, ferma restando l'esigenza dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato»[78].

[77] Garante per la protezione dei dati personali, *Sistema automatico di ricerca dell'identità di un volto*, 26 luglio 2018, n. 440, doc. web n. 9040256, in www.garanteprivacy.it

[78] Garante per la protezione dei dati personali, *Sistema automatico di ricerca dell'identità di un volto*, 26 luglio 2018, n. 440, doc. web n. 9040256, in www.garanteprivacy.it

In particolare, è stato messo in rilievo, come, secondo il medesimo decreto attuativo della direttiva Europea, ai sensi dell'art. 7, il trattamento delle informazioni biometriche sia consentito solo con una base normativa e garanzie adeguate e solo se strettamente necessario, requisito soddisfatto da diverse disposizioni regolamentari e legislative già in vigore, tra cui l'art. 349 del c.p.p. relativo all'identificazione, il quale pare avere un'impostazione tale da consentire l'utilizzo di un *software* come SARI *Enterprise;* e l'art. 213 c.p.p. e successivi in materia di ricognizioni fotografiche atipiche (qualora SARI venga utilizzato ai fini investigativi o probatori) nel procedimento penale; il requisito della stretta necessità del trattamento viene appagato dal fine investigativo che lo strumento persegue correlato all'attività di identificazione realizzata dalle forze dell'ordine.

Tale configurazione dell'applicativo potrebbe largamente aiutare gli operatori delle attività di contrasto data la rapidità nelle identificazioni.

Tuttavia, la possibilità che esso si avvalga di algoritmi non testati e certificati non dovrebbe essere concessa, in quanto risulterebbe ancor di più difficoltoso comprendere quali parametri l'algoritmo prende come Input per poi produrre l'Output, risultando quindi in un rischio incrementale di false individuazioni. Il capitolato tecnico andrebbe rivisto almeno in questo punto.

5. S.A.R.I. Real Time e il successivo parere del Garante

Dopo aver esaminato S.A.R.I. nella sua prima configurazione, pare opportuno analizzare l'applicativo anche nella versione *Real Time.*

Occorre premettere, che tale configurazione di S.A.R.I. non sembra essere ancora attiva all'interno dei confini italiani.

Utilizzato in questa versione S.A.R.I. è in grado di analizzare una grande quantità di volti inquadrati dalle telecamere, «collocate in luoghi specifici oggetto di osservazione e di confrontarli con un database più ristretto di persone ricercate (la c.d. "*watch-list"*), la cui grandezza è al massimo di 10.000 volti»[79] . La novità in questo scenario è rappresentata dalla possibilità di poter installare le videocamere direttamente in aree sensibili, al fine di utilizzare la tecnologia in modo più mirato «Il sistema consente, inoltre, di registrare i flussi video delle telecamere fungendo, in tal senso, quale attività di video sorveglianza»[80]. Aumentando l'effettivo supporto alle forze dell'ordine in materia di pubblica sicurezza, ma anche di indagine e prevenzione dei reati.

[79]J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in INTELLIGENZA ARTIFICIALE E PROCESSO PENALE: INDAGINI; PROVE E GIUDIZIO; a cura di G. Di Paolo, L. Presacco. P. 34

[80] Garante per la protezione dei dati personali, Parere sul sistema Sari Real Time, 25 marzo 2021, n. 127, doc. web n. 9575877, in www.garanteprivacy.it.

In tal senso, se l'algoritmo dovesse riscontrare una somiglianza tra l'immagine del volto ricercato ed il *frame* video analizzato, scatterebbe il c.d. *alert;* tale input viene utilizzato come una sorta di «campanello d'allarme», che richiama l'attenzione dell'operatore umano, il quale anche in questo caso viene chiamato a compiere l'ultimo passo, ovvero quello di confermare o smentire la decisione algoritmica. Potremmo quindi definire tale tecnologia come una videoripresa «potenziata».

Il Garante si è espresso, anche in relazione a S.A.R.I. *Real Time* dopo aver ricevuto da parte del Ministero dell'interno una bozza sul funzionamento di S.A.R.I. e una valutazione di impatto[81] di tale tecnologia.

Tale istruttoria conclusasi nel marzo 2021[82] ha avuto un esito opposto rispetto al primo provvedimento riguardante la versione *Enterprise* di S.A.R.I.: il Garante ha deciso di emettere un parere contrario in relazione all'impiego di S.A.R.I. *Real time*, anche considerando la sempre più crescente ondata di consapevolezza circa le possibili distorsioni compiute

[81] Linee-guida del Gruppo, Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248) in Valutazione d'impatto della protezione dei dati (DPIA) - Garante Privacy "Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato."

[82] Garante per la protezione dei dati personali, Parere sul sistema Sari Real Time, 25 marzo 2021, n. 127, doc. web n. 9575877, in www.garanteprivacy.it.

dai sistemi basati sull'IA[83]. Il sistema in argomento realizzerebbe, infatti, «un trattamento automatizzato su larga scala che può riguardare, tra l'altro, anche coloro che siano presenti a manifestazioni politiche e sociali, che non sono oggetto di "attenzione" da parte delle forze di Polizia [...] Pertanto, si determina una evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui.»[84]. Sembrerebbe quindi realizzare una vera e propria forma di sorveglianza di massa: con riferimento alle manifestazioni pubbliche, il sistema è in grado di raccogliere sia i dati biometrici di cui all'art. 9 GDPR, ossia quei dati in grado di identificare una persona fisica in modo univoco, sia altre categorie di dati sensibili, come quelli in grado di indicare, ad esempio, l'appartenenza sindacale e l'orientamento politico. Inoltre, l'art. 9 GDPR richiede che il trattamento in oggetto debba essere previsto dall'Unione Europea o dalla legge di uno stato membro, al riguardo il Garante ha precisato che: «nella documentazione fornita dal Ministero dell'Interno e tra le fonti normative da questo indicate non si rinviene alcuna disposizione specifica che consenta tale tipo di

[83] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in INTELLIGENZA ARTIFICIALE E PROCESSO PENALE: INDAGINI; PROVE E GIUDIZIO; a cura di G. Di Paolo, L. Presacco. P. 36

[84] Garante per la protezione dei dati personali, Parere sul sistema Sari Real Time, 25 marzo 2021, n. 127, doc. web n. 9575877, in www.garanteprivacy.it.

trattamento. In particolare, il Decreto, ancorché preveda in astratto tali trattamenti, non può considerarsi, di per sé, fonte normativa idonea a legittimarli»[85], invece con riguardo alle categorie particolari di dati, deve sussistere un'adeguata base normativa idonea ad identificare modalità e presupposti d'uso, data la forte ingerenza nella vita privata di tale strumento[86]: «al riguardo è da osservare che tale base giuridica, in esito alla ponderazione di tutti i diritti e le libertà coinvolti, dovrà, tra l'altro, rendere adeguatamente prevedibile l'uso di tali sistemi, senza conferire una discrezionalità così ampia che il suo utilizzo dipenda in pratica da coloro che saranno chiamati a disporlo, anziché dalla emanata previsione normativa»[87].

In conclusione, secondo il Garante, S.A.R.I. nella sua versione *Real Time* è potenzialmente dannoso per la collettività: le video riprese finirebbero per raccogliere informazioni anche di soggetti non ricercati ed, in secondo luogo, per le inadeguate fondamenta normative. Pertanto, prima di essere adeguatamente impiegato al fine identificativo e di controllo,

[85] Ibidem

[86] bene giuridico tutelato anche dall'art. 8 della Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali che prevede che ogni persona ha diritto al rispetto della propria vita privata e familiare e 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 dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

[87] Garante per la protezione dei dati personali, Parere sul sistema Sari Real Time, 25 marzo 2021, n. 127, doc. web n. 9575877, in www.garanteprivacy.it.

bisognerebbe essere certi della sua capacità di individuare e distinguere un soggetto da un altro, al fine di evitare false individuazioni, ed allo stesso tempo assicurarsi che il sistema non sia affetto da *bias* in grado di discriminare minoranze o specifici gruppi di individui, oltre alla necessità di individuare forme di tutela adeguate per tutti quei soggetti inquadrati dalle telecamere, ma non ricercati, i cui dati biometrici vengono comunque elaborati.

6. Una stratificazione normativa

Giunti a questo punto, ed alla luce degli attuali sviluppi in materia di regolamentazione per quanto riguarda l'intelligenza artificiale[88], è necessario soffermarsi su alcune particolarità normative che caratterizzano la materia, ossia, il concorso tra diversi strumenti regolamentativi, (tra cui anche le fonti di *soft law)* nazionali e sovranazionali, dovuti alle peculiarità della tecnologia stessa ed ai soggetti coinvolti[89];

[88] Si allude all'AI Act dell'Unione Europea

[89] G. MOBILIO, Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative, in Ricerche giuridiche n.224, 2021.

In Italia, come già detto, le tecnologie di riconoscimento facciale non sono state adeguatamente collocate all'interno del Codice penale, non esistono infatti norme ad *hoc* che disciplinino tale tecnologia[90].

A livello politico, va però sottolineato che non sempre si è dimostrato disinteresse per quanto concerne i rischi legati alle tecnologie di riconoscimento biometrico a distanza, infatti, alcuni parlamentari hanno esposto dei quesiti al Governo[91], finalizzati a comprendere meglio l'effettivo funzionamento di SARI. Tali interrogazioni hanno portato poi ad una proposta di legge[92], la quale mirava a colpire i soggetti pubblici e privati i quali si armassero di telecamere «rafforzate» da sistemi di riconoscimento facciale in luoghi pubblici o aperti al pubblico, attraverso una moratoria: sfruttando tale meccanismo, sarebbe venuto alla luce un divieto di utilizzo di tale strumento anche da parte degli operatori di polizia, in attesa di un intervento legislativo ad *hoc* in grado di tutelare i diritti e le libertà degli individui.

Tuttavia, le cose non sono andate come auspicato. Nel momento in cui, il parlamento ha convertito il c.d. decreto capienze[93] , ha aggiunto una previsione alla proposta di legge presentata nell'aprile 2021, proprio con

[90] F. LO CHIATTO, Dati biometrici, riconoscimento facciale, tutela della privacy, 04 Luglio 2021, in www.datarpotectionlaw.it

[91] Si allude alle già citate interrogazioni parlamentari, On. Sensi, n. 3-02074 e dall'On. Ceccanti e altri n. 5-03432

[92] Proposta di legge A.C. n. 3009 presentata dal deputato Sensi il 12 aprile 2009

[93] D.l.. 8 ottobre 2021, n. 139, conv. con mod. dalla l. 3 dicembre 2021, n. 205

riguardo alla materia penale, tale misura, prevede all'art. 9 co. 9 un divieto temporaneo di utilizzo delle telecamere posto inizialmente fino a dicembre 2023 posticipato al 31 dicembre 2025[94], o fino ad un intervento legislativo specifico in materia di installazione e utilizzo di telecamere «potenziate». Ciononostante, la stessa disposizione al co.12 pondera un'eccezione: tale moratoria non si applica ai «trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali […] in presenza, salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero, di parere favorevole del Garante della privacy.»[95]

Sembra quindi che il parlamento abbia voluto consentire, a determinate istituzioni, come le forze di *law enforcement,* la possibilità di avvalersi pienamente di tali strumenti anche in modalità *Real Time,* salvo l'autorizzazione da parte del Garante della privacy.

Appare, però, che anche in questo caso la norma non possa superare il vaglio del criterio di proporzionalità imposto dagli artt. 7 e 8 della carta di

[94] Attraverso il D.L 51/2023

[95] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in INTELLIGENZA ARTIFICIALE E PROCESSO PENALE: INDAGINI; PROVE E GIUDIZIO; a cura di G. Di Paolo, L. Presacco. P.47

Nizza[96], requisiti necessari per il trattamento di dati biometrici, ed ancora, non viene indicato con chiarezza per che tipologie di reati tali strumenti possono essere utilizzati.

Difatti una simile eccezione sconvolgerebbe del tutto il senso dell'intervento parlamentare, che ha portato alla richiesta di una moratoria nei confronti di chi utilizzi videocamere alimentate da sistemi di IA. Questa mirava sostanzialmente a limitarne l'uso anche nel momento in cui fossero gli stessi operatori delle attività di contrasto ad utilizzarle.

Tale eccezione potrebbe avvalorare che, anche al netto della misura prevista dalla legge, gli operatori di polizia e gli accusatori in sede processuale, possano avvalersi di S.A.R.I. anche nella versione *Real Time* al fine dell'identificazione[97], tuttavia, l'impiego di SARI come strumento di individuazione e ricognizione algoritmica sembra rimanere ancora vietato dall'art 189 c.p.p.[98]. In relazione alle tutele poste per le libertà morali dell'individuo: la norma fa sì che, da un lato si rispettino i diritti fondamentali, dall'altro lato non si vuole pregiudicare l'accertamento della verità, tuttavia, è chiaro che i metodi di accertamento atipici come le

[96] L'art. 7 stabilisce che ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni.
L'art. 8 sancisce che ogni soggetto ha diritto alla protezione dei dati di carattere personale che lo riguardano.

[97] ai sensi dell'art. 349 c.p.p.

[98] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in INTELLIGENZA ARTIFICIALE E PROCESSO PENALE: INDAGINI; PROVE E GIUDIZIO; a cura di G. Di Paolo, L. Presacco. P. 47

tecnologie di riconoscimento facciale, possano alterare la capacità di ricostruzione del fatto, pertanto tali ricognizioni vengono vietate.

La conversione del decreto capienze e l'eccezione posta al comma 12 art. 9, pare essere l'intervento normativo ad oggi più consistente all'interno dei confini italiani in materia di nuove tecnologie ai fini preventivi e repressivi dei reati.

Dopo questa analisi è necessario spostare l'attenzione sul fronte euro-unitario, il quale ha dimostrato abilità decisamente migliori nel legiferare in materia di tecnologie di riconoscimento facciale e di protezione dei dati biometrici.

A livello sovranazionale, possiamo trovare diverse normative. Tra le più significative troviamo il *General Data Protection Regulation* 2016/679, *l'Artificial Intelligence Act* 2024/1689 ed anche la Carta Etica sull'utilizzo dei sistemi di intelligenza artificiale nei sistemi giudiziari e ambiti connessi del 2018.

Ponendo, in particolare, l'attenzione sull' *AI Act*, va sottolineato come, si tratti della prima normativa a livello globale in materia di intelligenza artificiale. Essa mira a diventare uno standard internazionale (come già avvenuto in passato in materia di protezione dei dati attraverso il Regolamento 2016/679 GDPR)

Il regolamento, proposto nel 2021 ed approvato nell'estate 2024, opera attraverso un approccio c.d. *risk based*[99], ossia orientato al rischio. In particolare, esso categorizza le tecnologie basate sull'intelligenza artificiale su quattro diversi livelli di rischio: da un rischio inaccettabile ad un rischio minimo o nullo. Nel primo scaglione di rischio, ovvero quello più elevato, rientrano gli strumenti in grado di riconoscere un volto a distanza in tempo reale, il social scoring ed in linea generale tutti i sistemi in grado di alterare la volontà umana.

In materia di riconoscimento facciale, il regolamento effettua una distinzione tra gli strumenti ad uso *live* (come la versione *Real time* di SARI) ed impiego post (come la versione *Enterprise*), sulla base dell'ingerenza nella vita privata dei cittadini di dette tecnologie[100].

All'interno del perimetro regolatorio, i sistemi di riconoscimento biometrico a distanza, come già detto, vengono racchiusi nel livello di rischio più alto, ossia inaccettabile[101]. Per questo motivo, essi vengono banditi all'interno dell'Unione[102]: tuttavia, il Consiglio europeo ha deciso di consentirne l'utilizzo, anche in modalità *live (c.d. Real Time)* alle forze

[99] M. BORGOBELLO, AI Act, da oggi è "ufficiale": come cambiano le regole per l'IA, 12 luglio 2024, in, www.agendadigitale.eu

[100] F. PAOLUCCI, *AI act e riconoscimento facciale: i rischi di delegare la questione agli stati membri* , 26 Aprile 2024, in www.agendadigitale.eu

[101] Il rischio viene detto inaccettabile perché contrario a tutti i valori e principi dell'Unione Europea: Democrazia, stato di diritto e il rispetto dei diritti fondamentali

[102] In linea generale, vengono considerati ad alto rischio o rischio inaccettabile, tutti i sistemi di AI in grado di profilare persone fisiche

di *law enforcement* in spazi accessibili al pubblico per attività di contrasto[103]. Al riguardo, il regolamento prevede una serie di eccezioni, ben definite, all'art. 5 paragrafo 1, lettera d):

«sono vietate le pratiche di IA seguenti:

l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di un sistema di IA per effettuare valutazione del rischio relative a persone fisiche al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità; tale divieto non si applica ai sistemi di IA utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa;»[104]

o ancora alla lettera h):

«l'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto a meno che, e nella misura in cui, tale uso sia strettamente necessario per uno degli obiettivi seguenti: | i) | la ricerca mirata di specifiche vittime di sottrazione,

[103] Tali eccezioni sono state fortemente richieste dal rappresentante francese, spalleggiato dall'omonimo spagnolo ed italiano, dopo i vari attentati subiti negli scorsi anni dalla Francia.

[104] Gazzetta Ufficiale dell'Unione Europea, Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio, 12 luglio 2024, che stabilisce regole armonizzate sull'intelligenza artificiale. V. 9/2024 - sistemapenale.it, https://www.sistemapenale.it/pdf_contenuti/1725281617_de-flammineis-fasc-92024.pdf.

tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; | ii) | la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; | iii) | la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale»[105].

Nonostante le eccezioni poste a favore delle forze di polizia, tali sistemi in modalità *Real Time,* come si può leggere al paragrafo 2 del medesimo articolo, devono essere utilizzati dalle forze dell'ordine come ausilio, al solo fine della conferma dell'identità del soggetto ricercato, prendendo in considerazione: la natura della situazione che dà luogo al possibile uso, la gravità, la probabilità e l'entità del danno in caso di mancato utilizzo dell'applicativo, ma anche, le conseguenze per i diritti e le libertà di tutti gli interessati.

Tali eccezioni vengono legittimate solamente nel momento in cui l'autorità di contrasto abbia completato una valutazione d'impatto sui

[105] tale previsione lascia comunque impregiudicato l'articolo 9 GDPR - trattamento di categorie particolari di dati - per quanto riguarda il trattamento di dati biometrici a fini diversi dell'attività di contrasto

diritti fondamentali, come previsto dall'art. 27[106], ed il sistema utilizzato sia correttamente registrato nella banca dati UE conformemente all'art 49[107].

Inoltre, l'utilizzo di tali sistemi è subordinato ad un'autorizzazione che dovrà essere emanata dall'autorità giudiziaria o amministrazione indipendente competente, in conformità al diritto nazionale vigente[108]. Tale autorità potrà permettere l'utilizzo del sistema nel solo caso in cui questo impiego risulti necessario e lo strumento proporzionale al fine.

Essa dovrà poi notificare l'autorizzazione all'autorità di vigilanza del mercato e all'autorità nazionale per la protezione dei dati.

Per quanto riguarda invece le fonti di *soft law*[109] *,* troviamo la Carta etica sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi del 2018. Tale normativa adottata dall*' European Commission for the Efficiecy of Justice CEPEJ*, anche se non vincolante, vuol far sì che l'IA venga applicata in ambito giudiziario in modo responsabile e nel rispetto dei diritti fondamentali. Essa enuncia alcuni

[106] La valutazione dovrà contenere, ad esempio: i possibili soggetti interessati, i rischi specifici di danno che possono incidere sulle persone fisiche o sui gruppi di persone individuati, l'attuazione di misure di sorveglianza umana, le misure da adottare nel momento in cui tale rischio si concretizzasse

[107] Tuttavia, in casi di particolare urgenza, è possibile procedere anche senza iscrizione ex ante, a condizione che tale registrazione sia completata senza indebito ritardo

[108] Anche in questo caso, in situazioni di urgenza, si potrà procedere all'utilizzo, la richiesta all'autorità giudiziaria dovrà essere presentata entro le 24 ore successive, e nel caso di diniego, l'utilizzo dovrà essere interrotto con effetto immediato, e tutti i dati raccolti nonché gli output prodotti dovranno essere eliminati

[109] norme di carattere non vincolante

principi che: «dovrebbero essere sottoposti a regolare applicazione, monitoraggio e valutazione da parte di attori pubblici e privati»[110]. La Carta rappresenta per noi un'importante atto normativo, in quanto vaglia anche il tema della giustizia predittiva e dell'utilizzo di modelli statistici ai fini di aumentare la prevedibilità degli esiti giudiziari, ma sembra potersi applicare anche alla prevenzione e repressione dei reati.

I principi enunciati dalla Carta sono:

i) Principio del rispetto dei diritti fondamentali, il quale mira ad assicurare che l'elaborazione e l'attuazione di strumenti e servizi di intelligenza artificiale siano compatibili con i diritti fondamentali: «Il trattamento di decisioni e dati giudiziari deve avere finalità definite chiaramente, che rispettino i diritti fondamentali garantiti dalla Convenzione europea sui diritti dell'uomo CEDU». In particolare, dev'essere assicurato il diritto di accesso ad un giudice e ad un equo processo.[111]

ii) Principio di non discriminazione, che vuole prevenire lo sviluppo e l'intensificazione di qualsiasi discriminazione. Date le particolarità di tale tecnologia, spesso in grado di: «rivelare le

[110] COMMISSIONE EUROPEA PER L'EFFICENZA DELLA GIUSTIZIA (CEPEJ), Carta etica per l'uso dell'intelligenza artificiale nei sistemi giudiziari e nei loro ambiti connessi, Strasburgo, 3 dicembre 2018. Pag. 5

[111] COMMISSIONE EUROPEA PER L'EFFICENZA DELLA GIUSTIZIA (CEPEJ), Carta etica per l'uso dell'intelligenza artificiale nei sistemi giudiziari e nei loro ambiti connessi, Strasburgo, 3 dicembre 2018. Pag. 7

discriminazioni attraverso raggruppamento o la classificazione di dati», dev'essere infatti adottata una particolare vigilanza, specialmente nel momento in cui il trattamento riguardi dati sensibili.[112]

iii) Principio di qualità e sicurezza, i creatori di modelli di IA ad apprendimento automatico dovrebbero poter far ricorso alle competenze degli esperti e professionisti del sistema giustizia, al fine di produrre modelli funzionali, che permettano di ottenere il miglior risultato e di condividere adeguate salvaguardie etiche.[113]

iv) Principio di trasparenza, imparzialità ed equità, il quale mira a raggiungere un equilibrio tra le proprietà intellettuali di alcune metodologie di trattamento e l'esigenza di trasparenza, imparzialità ed equità, ad esempio attraverso la limitazione dei segreti industriali.[114]

v) Principio del "controllo da parte dell'utilizzatore", che punta ad assicurare che gli utilizzatori siano attori informati e abbiano

[112] COMMISSIONE EUROPEA PER L'EFFICENZA DELLA GIUSTIZIA (CEPEJ), Carta etica per l'uso dell'intelligenza artificiale nei sistemi giudiziari e nei loro ambiti connessi, Strasburgo, 3 dicembre 2018. Pag. 8

[113] COMMISSIONE EUROPEA PER L'EFFICENZA DELLA GIUSTIZIA (CEPEJ), Carta etica per l'uso dell'intelligenza artificiale nei sistemi giudiziari e nei loro ambiti connessi, Strasburgo, 3 dicembre 2018. Pag. 10

[114] COMMISSIONE EUROPEA PER L'EFFICENZA DELLA GIUSTIZIA (CEPEJ), Carta etica per l'uso dell'intelligenza artificiale nei sistemi giudiziari e nei loro ambiti connessi, Strasburgo, 3 dicembre 2018. Pag. 11

controllo delle loro scelte: «I professionisti del sistema giustizia dovrebbero essere in grado, in qualsiasi momento, di rivedere le decisioni giudiziarie e i dati utilizzati»[115]

Si può desumere che la Commissione voglia esprimere un approccio di prudenza in relazione all'introduzione dei sistemi di IA negli ambiti giudiziari. Tale approccio è dovuto al delicatissimo compito che tale settore ricopre all'interno di una società civile.

Anche in questo caso la *ratio* della Carta è rappresentata dal rispetto dei diritti fondamentali; come già si è visto in precedenza anche per il Regolamento 2024/1689 EU.

Alla luce di quanto detto finora possiamo affermare che il quadro normativo sovranazionale risulti più in linea con i bisogni attuali del settore giustizia: lo schema normativo composto sia da fonti vincolanti, che da fonti di *soft law,* sembra poter dare ora un'effettiva sicurezza agli operatori nell'utilizzare sistemi basati sull'IA, inclusi i sistemi di riconoscimento facciale.

Resta comunque problematica, almeno all'interno dei confini italiani l'implementazione di misure che accompagnino l'*AI Act* verso la sua

[115] COMMISSIONE EUROPEA PER L'EFFICENZA DELLA GIUSTIZIA (CEPEJ), Carta etica per l'uso dell'intelligenza artificiale nei sistemi giudiziari e nei loro ambiti connessi, Strasburgo, 3 dicembre 2018. Pag. 12

applicazione totale[116]. Fermo restando che si tratta di un Regolamento Europeo, il quale a livello normativo non richiede particolari misure implementative da parte degli stati membri, si è visto come, spesso il Regolamento si rimetta alle norme interne di ciascun stato membro. È quindi auspicabile un intervento legislativo, che, da anni viene richiesto, in grado di soddisfare e sfruttare al meglio la normativa offerta dal Regolamento 2024/1689.

7. L'impatto sui diritti fondamentali

La domanda che ora sorge spontanea è la seguente: quali sono i diritti fondamentali che vengono tutelati in materia di riconoscimento biometrico a distanza mediante questi atti normativi? In questo paragrafo ne valuteremo alcuni.

In primo luogo, il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza: «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

[116] Entro fine 2026

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 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, e nella stessa stesura letterale, l'art. 8 Convenzione Europea dei Diritti dell'uomo)

Tuttavia, l'intrusione nella vita privata del soggetto, si verifica attraverso una compressione sostanziale della privacy. L'interferenza con il diritto al rispetto della vita privata avviene mediante l'utilizzo dei sistemi di riconoscimento biometrico a distanza, come conseguenza, ancora una volta, del vuoto normativo che caratterizza tali tecnologie nel nostro ordinamento, rendendo ogni utilizzo dello strumento illegittimo, se non nei modi e limiti previsti dalle precedenti eccezioni, come ad esempio, il comma 12 dell'art. 9 D.lgs. 51/2018 che rende l'utilizzo legittimo per gli operatori di *law enforcement* per fini preventivi e repressivi dei reati.

In secondo luogo, la lesione del diritto alla tutela della dignità umana; soprattutto in relazione alla sua attività *live,* tale tecnologia: «può evidentemente tradursi in occasioni di sorveglianza di massa»[117]. Questa

[117] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in Ricerche giuridiche n.224, 2021, pag. 78

capacità di riprendere un numero indefinito di soggetti e di azioni che gli individui conducono, anche di quei soggetti non coinvolti in particolari ricerche e del tutto estranei, può risultare in una lesione della loro sfera personale, essendo queste vittime di una illegittima acquisizione di dati personali[118].

L'assenza del consenso dell'interessato, che coinvolge il diritto alla riservatezza e alla protezione dei dati personali (si pensi, ad esempio, alle attività di prevenzione svolte durante le manifestazioni). Le acquisizioni dei dati degli interessati, avviene in difetto di un previo consenso dell'interessato, «il quale è così spogliato di qualsiasi potere sul controllo della circolazione dei propri dati»[119]. Il consenso dell'interessato in materia di trattamento di dati biometrici, dev'essere generalmente sempre raccolto. In conformità al GDPR esso dev'essere esplicito ed informato al fine di poter dare la possibilità all'interessato di richiedere informazioni al titolare del trattamento. Tuttavia, sussistono alcune eccezioni a tale obbligo, come la necessità di adempiere ad attività di interesse pubblico. Sembra quindi essere legittimo il trattamento in assenza del consenso dell'interessato per la mera identificazione di un soggetto ricercato, ma

[118] E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?* in Diritto Penale e Uomo, Milano, 19 maggio 2021, fascicolo 5/2021, pag. 11
[119] Ibidem

non per quanto riguarda il controllo generale di aree sensibili come manifestazioni pubbliche.

Quando poi, il trattamento dei dati biometrici avviene nell'ambito di un procedimento penale, può essere compromesso il diritto ad un equo processo. Il rischio è rappresentato dalla possibilità che i dati raccolti possano essere utilizzati per avviare un'indagine o limitare la libertà personale di un soggetto. Il problema di fondo è rappresentato, oltre che dall'opacità di tali sistemi nei processi decisionali[120], anche dal tasso di errore che li caratterizza, percentuale che diventa inaccettabile nel momento in cui si limita la libertà personale di un individuo[121].

Il dibattito sul bilanciamento tra l'utilizzo di nuove tecnologie come gli strumenti di riconoscimento facciale e le implicazioni per i diritti fondamentali rimane aperto, anche a fronte degli sviluppi normativi che sono stati fatti nell'eurozona. Ciononostante, sembra plausibile restringere i diritti fondamentali a fronte di specifiche esigenze, al fine di salvaguardare interessi di pari rango o superiori, come la necessità di salvaguardare la pubblica sicurezza o la necessità di effettuare un'attività di prevenzione dei reati: «Tuttavia, la prevalenza degli uni sugli altri non

[120]In contrasto, inoltre, con l'art. 15 GDPR ossia il diritto di accesso riconosciuto in capo all'interessato, il quale ha la il diritto di essere informato dal titolare del trattamento se è in corso un trattamento dei propri dati personali e di poter accedere a questi

[121] E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?* in Diritto Penale e Uomo, Milano, 19 maggio 2021, fascicolo 5/2021, P. 12-13

può essere decretata una volta per tutte in modo definitivo: non esistono criteri oggettivi e matematici, ma il risultato del bilanciamento è spesso frutto dell'applicazione di criteri elastici come quello di proporzione, necessità e *extrema ratio»*[122]

[122] E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?* in Diritto Penale e Uomo, Milano, 19 maggio 2021, fascicolo 5/2021, P.14

CAPITOLO III:
PROSPETTIVE FUTURE E CONCLUSIONI FINALI

In conclusione, tali nuove tecnologie, ricche di aspetti positivi quanto negativi, che in un futuro prossimo mirano a diventare anche all'interno del procedimento penale italiano uno strumento di ricerca della prova, di ricognizione personale e di individuazione, rischiano a livello normativo nazionale di rimanere incomprese[123], anche in relazione al lavoro fatto sinora dal Parlamento in merito alla conversione del D.lg. Capienze nella legge n. 201 del 2018: lo strumento attraverso il quale si è deciso di legiferare offre tempistiche troppo brevi, non consone a disciplinare con cautela rispetto a tecnologie così delicate sotto tutti i punti di vista. Diviene quindi imprescindibile un provvedimento normativo coordinato, sia sul piano giuridico sia su quello tecnico[124], al fine di risolvere le criticità che caratterizzano tale strumento[125].

[123] Si fa riferimento al vuoto normativo che caratterizza la materia. Tale carenza comporta difatti la mancata possibilità di sfruttare questa tecnologia al meglio.

[124] Ovvero quell'ambito prettamente di ricerca e sviluppo, che rende possibile il miglioramento di tali tecnologie.

[125] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in INTELLIGENZA ARTIFICIALE E PROCESSO PENALE: INDAGINI; PROVE E GIUDIZIO; a cura di G. Di Paolo, L. Presacco. P. 50

L'approccio dovrebbe essere duplice a seconda che si tratti di tecnologie di *facial recognition* impiegate per la prevenzione e la repressione dei reati, o per altri scopi. Quanto alle prime occorrerebbe approntare una normativa minuziosa, che definisca, ad esempio, per quali tipologie di reati queste tecnologie possano essere impiegate, quali garanzie debbano essere rispettate[126] e come gli algoritmi debbano essere allenati. Al tempo stesso, sembra però necessaria una certa flessibilità normativa per intervenire in modo efficace, ed apportare modifiche che saranno sicuramente necessarie e che daranno la possibilità di garantire una normativa pertinente e aggiornata.[127]A tal proposito è noto che: «a fronte dell'importanza strategica assunta dalle moderne tecnologie del controllo, l'ordinamento processuale italiano risulta ancora affetto da previsioni datate e da gravissime lacune normative, non essendo stati regolati [...] neppure istituti classici come le semplici videoriprese investigative»[128]. Si rivela quindi necessario anche un cambio di paradigma in merito alle nuove tecnologie.

[126] Ad esempio, per quanto tempo le immagini possono essere conservate dagli operatori di polizia.

[127] Approccio che tra l'altro è stato adottato anche a livello europeo in sede normativa nel momento in cui fu deciso come procedere per quanto concerne l'*AI act.* Una possibilità potrebbe essere rappresentata dall'utilizzo di clausole aperte regolamentari. Le quali però non dovrebbero essere applicate ad aspetti particolarmente delicati della disciplina.

[128] J. DELLA TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?* in INTELLIGENZA ARTIFICIALE E PROCESSO PENALE: INDAGINI; PROVE E GIUDIZIO; a cura di G. Di Paolo, L. Presacco. P.52

Dall'altro lato per quanto riguarda invece gli strumenti di *facial recognition,* non utilizzati al fine di prevenire e reprimere i reati[129],(si pensi alle declinazione di tali tecnologie utilizzate, ad esempio, per gestire gli accessi in alcuni edifici o all'integrazione di esse negli *smartphone*), è corretto suppore che, attraverso una normativa minuziosa troppo complessa e rigida, si corra il rischio di rallentare gli operatori economici e lo sviluppo, aumentando a questi il carico burocratico e limitando così anche la competitività a livello globale. Sarebbe quindi corretto adottare una normativa differente, più flessibile, almeno nel caso concreto in cui i diritti fondamentali non siano a rischio.

Un altro aspetto dove si evidenziano ampie possibilità di perfezionamento è l'assenza di trasparenza che caratterizza il funzionamento interno di tali tecnologie. Come si è visto in relazione al restringimento dei diritti fondamentali per tutelare interessi di pari rango o superiori, potremmo ipotizzare una simile applicazione anche ai segreti industriali[130] , comprimendo alcuni interessi di terzi si potrebbe almeno in sede processuale, in presenza di determinati requisiti, arrivare a comprendere meglio il funzionamento di determinati *tools* aumentando così

[130]Anche nel rispetto del principio di trasparenza, equità e correttezza della Carta etica

l'accuratezza nella creazione ed applicazione delle norme[131] come conseguenza di una comprensibilità più elevata della tecnologia.

Inoltre, dati gli alti rischi per i diritti degli individui coinvolti, sarebbe opportuno allargare il dibattito politico anche ad altri portatori di interesse, come rappresentanti sindacali, esperti ed associazioni di cittadini, al fine di dare pieno esercizio a questi dei loro diritti civili e politici, essendo così in grado di comprendere le posizioni di chi sarebbe poi vittima di tali strumenti, evitando di alimentare discussioni controverse, che ad esempio, qualche anno fa sono sorte in Francia in seguito all'approvazione della legge sulla sicurezza globale, la quale concedeva alle forze di polizia di utilizzare senza limite la rete di videosorveglianza e strumenti di videosorveglianza intelligente presenti all'interno dei confini francesi[132].

Il legislatore nei prossimi anni troverà sempre più sfide regolative legate al mondo delle nuove tecnologie, è pertanto necessario che questi si impegni nella profonda comprensione delle potenzialità ma soprattutto dei limiti e delle criticità di suddette applicazioni, al fine di non ritrovarsi succubi di un progresso inevitabile.

[131] Una conoscenza più consapevole della tecnologia in esame porterebbe in primo luogo il legislatore a formulare leggi più precise in grado di affrontare problematiche specifiche, in secondo luogo il giudice a ponderare decisioni più consapevoli ed informate.

[132] F. DE SIMONE, Una nuova tipologia di prevenzione: algoritmi, intelligenza artificiale e riconoscimento facciale, in Archivio Penale 2023, n.2. P.32

BIBLIOGRAFIA

- *Algoritmo - Enciclopedia Treccani*. Available at: https://www.treccani.it/enciclopedia/algoritmo/ (Accessed: 20 July 2024).

- Baiocco, L., Ferri, E. and Celsi, L.R. (2022) *Riconoscimento Facciale Automatico: Opportunità e minacce*, *AI4Business*. Available at:

- Basile, F. (2019) *Intelligenza artificiale e diritto penale: Quattro possibili Percorsi di Indagine*, *Diritto Penale e Uomo*. Available at: https://air.unimi.it/handle/2434/680633 (Accessed: 23 July 2024).

- Bennett Moses, L. and Chan, J. (2016) 'Algorithmic prediction in policing: Assumptions, evaluation, and Accountability', *Policing and Society*, 28(7), pp. 806–822. doi:10.1080/10439463.2016.1253695.

- Borgobello, M. (2024) *Ai Act, da Oggi è 'ufficiale': Come cambiano le regole per l'ia*, *Agenda Digitale*. Available at: https://www.agendadigitale.eu/cultura-digitale/ai-act-da-oggi-e-ufficiale-come-cambiano-le-regole-per-lia/#:~:text=Il%20Regolamento%20europeo%202024/1689%20%E2%80%93%20noto%20come%20AI%20Act%20%E2%80%93 (Accessed: 13 September 2024).

- Carbone, M.R. (2021) *Sari, il riconoscimento facciale nella pubblica sicurezza: Servono Regole e trasparenza*, *Agenda Digitale*. Available at: https://www.agendadigitale.eu/sicurezza/privacy/sari-vantaggi-e-rischi-del-riconoscimento-facciale-nella-pubblica-sicurezza/#:~:text=Anche%20l%E2%80%99Italia%20ha%20sistemi%20di%20riconoscimento%20facciale:%20il%20sistema,%20gi%C3%A0#:~:text=A

nche%20l%E2%80%99Italia%20ha%20sistemi%20di%20riconoscimento%20facciale:%20il%20sistema,%20gi%C3%A0 (Accessed: 10 July 2024).

- Cath, C. *et al.* (2017) 'Artificial Intelligence and the "Good Society": The US, EU, and UK approach', *Science and Engineering Ethics* [Preprint]. doi:10.1007/s11948-017-9901-7.

- Currao, E. (2021) *Il riconoscimento facciale e i diritti fondamentali: Quale Equilibrio?*, *DPU | Diritto Penale e Uomo*. Available at: https://dirittopenaleuomo.org/contributi_dpu/il-riconoscimento-facciale-e-i-diritti-fondamentali-quale-equilibrio/#:~:text=Abstract.%20L%E2%80%99utilizzo%20sempre%20pi%C3%B9%20diffuso%20dei%20sistemi%20di%20intelligenza%20artificiale, (Accessed: 23 August 2024).

- De Simone, F. (2023) *Una Nuova Tipologia di Misure di Prevenzione: Algoritmi, Intelligenza Artificiale e Riconoscimento Facciale*, *Archivio Penale*. Available at: https://archiviopenale.it/una-nuova-tipologia-di-misure-di-prevenzione-algoritmi-intelligenza-artificiale-e-riconoscimento-facciale/articoli/40550#:~:text=Nel%20tentativo%20di%20ampliare%20gli%20strumenti%20di%20contrasto%20e%20garantire (Accessed: 04 September 2024).

- Della Torre, J. (2023) in *Ragioni Comuni 2019-2020*. Trieste, Italia: *Algoritmi di facial recognition e procedimento penale italiano*, pp. 167–181.

- Di Paolo, G., Presacco, L. and Della Torre, J. (2022) in *Editoriale Scientifica*. Napoli, Italia: INTELLIGENZA ARTIFICIALE E PROCESSO PENALE INDAGINI, PROVE, GIUDIZIO, pp. 7–60.

- Di Paolo, G., Presacco, L. and Lasagni, G. (2022) in *Editoriale Scientifica*. Napoli, Italia: INTELLIGENZA ARTIFICIALE E PROCESSO PENALE INDAGINI, PROVE, GIUDIZIO, pp. 63–90.

- Garante per la protezione dei dati personali (201 8) *Sistema automatico di Ricerca dell'identità di un volto - 26 luglio 2018 [9040256]*. Available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9040256 (Accessed: 24 August 2024).

- Garante per la protezione dei dati personali (2021) *Parere sul Sistema Sari real time - 25 marzo 2021 [9575877]*. Available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877 (Accessed: 24 August 2024).

- Girardi, S. (2021) *Dati biometrici. Quo vadis per un trattamento legittimo?*, *altalex*. Available https://www.altalex.com/documents/news/2021/04/23/dati-biometrici-quo-vadis-per-un-trattamento-legittimo (Accessed: 05 August 2024).

- Kostoris, R.E. (2021)*: Predizione Decisoria diversion processuale E archiviazione*, *www.sistemapenale.it*. Available at: https://www.sistemapenale.it/it/articolo/kostoris-predizione-decisoria-diversion-processuale-archiviazione (Accessed: 05 August 2024).

- Kostoris, R.E. (2024): *Intelligenza Artificiale, Strumenti predittivi e Processo Penale*, *Discrimen*. Available at: https://discrimen.it/intelligenza-artificiale-strumenti-predittivi-e-processo-penale/ (Accessed: 12 July 2024).

- Lavecchia, V. (2022) *Caratteristiche e Differenza Tra Face detection e face recognition in Informatica*, *Informatica e Ingegneria Online*. Available at: https://vitolavecchia.altervista.org/caratteristiche-e-differenza-tra-face-detection-e-face-recognition-in-informatica/ (Accessed: 05 August 2024).

- Lo Chiatto, F. (2021) *Dati biometrici, Riconoscimento facciale, tutela della privacy*, *Data Protection Law | Privacy e protezione dati personali*. Available at: https://www.dataprotectionlaw.it/2021/07/04/dati-biometrici-riconoscimento-facciale-tutela-della-privacy/#:~:text=Tra%20i%20dati%20biometrici%20di%20rilevante%20importanza%20risulta%20essere%20il (Accessed: 07 September 2024).

- Marinoni, P. (2024) *Human in the Loop, l'uomo al Centro dell'algoritmo*, *AI news*. Available at: https://ainews.it/human-in-the-loop-luomo-al-centro-dellalgoritmo/#:~:text=Con%20l'evoluzione%20dell'AI,%20%C3%A8%20importante%20considerare%20le%20implicazioni%20etiche%20del (Accessed: 16 July 2024).

- Maugeri, A.M. (2021) 'L'uso di Algoritmi predittivi per accertare La pericolosità sociale : Una sfida tra evidence-based practices e tutela dei diritti fondamentali', *Archivio penale*, (1), p. 12. doi:10.12871/97888331809771.

- Mobilio, G. (2021) *Tecnologie di Riconoscimento Facciale: Rischi per i diritti fondamentali e sfide Regolative*. Napoli, Italia: Editoriale Scientifica.

- Paolucci, F. (2024) *Ai Act E Riconoscimento Facciale: I rischi di delegare la questione agli stati membri*, *Agenda Digitale*. Available at: https://www.agendadigitale.eu/cultura-digitale/ai-act-e-riconoscimento-facciale-i-rischi-di-delegare-la-questione-agli-stati-membri/#:~:text=La%20norma%20in%20questione%20promette%20di%20regolare%20gli%20utilizzi%20di (Accessed: 27 August 2024).

- Valeri, M. (2022) *Mettiamoci La Faccia*, *Polizia di stato*. Available at: https://poliziamoderna.poliziadistato.it/articolo/3536228dc7e38a8916585953 1#:~:text=Piazza%20Duomo%20e%20dintorni%20sono%20gremiti%20da%20persone%20scese%20in (Accessed: 07 August 2024).