Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

a.a. 2023/2024

Intelligenza artificiale e dati biometrici: i sistemi automatici di riconoscimento facciale tra tutela della privacy, esigenze investigative e logiche di mercato

Relatore: Chiar.mo Prof. Massimo Bolognari

Studente: Cristina Bessega

Matricola 2021603

INDICE

INTRODUZIONE

Questa tesi nasce dalla volontà di rispondere ad un quesito di fondamentale: la prova ottenuta mediante riconoscimento facciale può essere utilizzata in un processo penale?

Nel presente elaborato si tenterà di dare una risposta a tale domanda, analizzando presentando i aspetti e le novità rilevanti in merito all'utilizzo combinato di tecnologie di riconoscimento biometrico e intelligenza artificiale legati a utilizzi commerciali e nel processo penale.

L'analisi seguirà una struttura divisa in tre capitoli. Nel primo sarà affrontato il tema dell'Intelligenza Artificiale, della sua definizione e delle questioni legislative di maggior rilievo, sia nell'utilizzo dell'IA a supporto del processo penale, sia legate ai potenziali rischi che questa può configurare, in particolare i rischi collegati alla tutela della privacy.

Nel secondo capitolo vengono presentati gli strumenti di riconoscimento biometrico, dai più utilizzati alle ultime innovazioni tecnologiche.
Questi strumenti hanno portato in diversi livelli a legiferare sull'utilizzo dei dati raccolti e sulla metodologia di raccolta, ma non solo. Saranno dunque presentati anche i principali aspetti legislativi in merito.

All'interno del terzo ed ultimo capitolo il tema centrale saranno le tecniche di riconoscimento facciale, partendo dalla sfera della sicurezza pubblica arrivando ad esempi di utilizzi più innovativi di questa tecnologia, in particolare verranno riportati degli esempi di utilizzo nel settore commerciale. Un'ulteriore aspetto cruciale verrà affrontato alla fine di tale capitolo, ossia l'uso del dato biometrico come prova all'interno del processo penale.

Capitolo I: Intelligenza artificiale e diritto penale

1. Premessa

All'interno del seguente capitolo verranno descritte le caratteristiche principali dell'Intelligenza Artificiale: partendo da una riflessione sulla natura stessa dell'intelligenza umana verrà esaminato come diverse discipline, dalla filosofia alla psicologia, abbiano tentato di definire e misurare questa complessa materia. Successivamente, si entrerà nell'ambito dell'intelligenza artificiale, analizzando come gli studiosi abbiano cercato di riprodurre artificialmente le caratteristiche distintive dell'intelligenza umana, come l'apprendimento, il ragionamento e la capacità di risolvere problemi. Esploreremo le origini storiche dell'IA, i suoi principi fondamentali e le sue più recenti evoluzioni. Infine, discuteremo delle leggi che regolamentano questo tema, delle implicazioni etiche e legali dell'intelligenza artificiale, con particolare attenzione alla privacy e alla tutela dei dati personali.

2. Intelligenza Artificiale: caratteristiche generali

Per affrontare il tema dell'Intelligenza Artificiale è necessario partire da ciò che rappresenta l'intelligenza, per poi analizzare come essa possa essere simulata artificialmente. Non esiste una definizione univoca di intelligenza. L'*Oxford Companion to the Mind*[1] apre la descrizione della voce "intelligence" con: "sono disponibili innumerevoli test per misurare l'intelligenza, ma nessuno sa con sicurezza che cosa sia l'intelligenza, e addirittura nessuno sa con sicurezza che cosa misurino i test disponibili".[2]

Varie discipline hanno tentato di definire il concetto di intelligenza come ad esempio la filosofia, la matematica, l'economia, la medicina, la psicologia, la linguistica. L'intelligenza umana, intesa come insieme di capacità cognitive, può essere dimostrata nella flessibilità di adattamento a nuovi contesti, nell'apprendimento continuo dall'esperienza, nella percezione della realtà, nell'intuizione, nel pensiero astratto, nell'ottimizzazione delle risorse e nella comunicazione efficace. Tutte queste caratteristiche, anche se diverse tra loro, convergono

[1] L'*Oxford Companion to the Mind* è un'opera di riferimento enciclopedica sulla mente umana, pubblicata per la prima volta nel 1987. Curata da Richard L. Gregory, noto psicologo e scienziato cognitivo, l'opera offre una panoramica completa e accessibile di tutti gli aspetti della mente, dal cervello alla coscienza, dalla percezione all'intelligenza artificiale.

[2] R. L. Gregory, «*Intelligence*», in *The Oxford Companion to the Mind*, a cura di R. L. Gregory, Oxford University Press, 1987, p. 375-379, p. 375. Testo originale: "*Innumerable tests are available for measuring intelligence, yet no one is quite sure of what intelligence is, or even of just what is that the available tests are measuring*

verso un comune denominatore, ossia la capacità di migliorare le proprie prestazioni attraverso l'acquisizione, l'elaborazione e l'applicazione delle informazioni.[3]

L'Intelligenza Artificiale prende ispirazione da tutte queste discipline, tentando di far replicare tale minimo comun denominatore ad una macchina: non si tratta dunque del solo studio dell'intelligenza ma della sua creazione, cioè la possibilità di creare artefatti intelligenti.

Possiamo ricondurre la nascita dell'espressione "intelligenza artificiale" a John Mc Carthy, divenuto in seguito uno dei padri fondatori dell'IA, il quale all'interno di un convegno da lui organizzato in materia di IA fece la seguente premessa:

"*Si tenterà di scoprire come si possa fare in modo che le macchine usino il linguaggio, formulino astrazione e concetti, risolvano tipi di problemi ora riservati agli esseri umani, e migliorino sé stesse*"[4].

Circa 30 anni dopo le affermazioni di Mc Carthy iniziarono a Diffondersi gli studi di Roger Schank, divenuto in seguito uno dei massimi teorici dell'Ia e tra I fondatori del linguaggio computazionale. Schank definì 5 attributi attraverso i quali riconoscere l'esistenza di un' IA: "*la capacità di comunicazione; la ossia tesa al perseguimento di un fine; infine, l'esistenza di un apprezzabile grado di creatività, intesa come capacità di assumere decisioni alternative laddove il piano di azione iniziale fallisca o non sia realizzabile*".[5]

Tutto ciò riconduce ad una caratteristica tipica dell'IA ossia il cosiddetto apprendimento automatico (c.d. *machine learning*), la predisposizione sviluppata da una macchina ad apprendere in maniera autonoma attraverso l'analisi dei dati senza istruzioni ben definite da parte dei programmatori, una tecnica che in seguito vedremo diventare sempre più utilizzata in una vasta gamma di settori.

Negli ultimi anni diversi studi hanno cercato di comprendere il comportamento della macchina nella relazione tra essa e il suo ambiente. Queste ricerche hanno evidenziato alcuni tratti dell'intelligenza che non sono riconducibili al ragionamento in senso stretto come la percezione e la capacità di esplorare attivamente l'ambiente. [6] In particolare, un contributo rilevante in

[3] Sartor, G. (2022). *L'intelligenza artificiale e il diritto* (1a ed.). Giappichelli
[4] da: *a proposal for the dartmouth summer research project on artificial intelligence* di J.McCarthy
[5] R.C. Schank, What's IA, Anyway?, in IA Magazine, Winter 8(4), 1987, pp. 59 ss.
[6] Sartor, G. (2022). *L'intelligenza artificiale e il diritto* (1a ed.). Giappichelli.

merito al rapporto tra intelligenza e ambiente è quello formulato da Rodney Brooks, figura di spicco nel campo della robotica comportamentale e fondatore di *iRobot*, azienda nota a livello mondiale per aver creato *Roomba*, l'ormai noto aspirapolvere robot. Brooks è noto per i suoi studi nell'ambito dell'Intelligenza Artificiale e all'interno del suo articolo del 1990 intitolato *"Elephants Don't Play Chess"*[7] scriveva:

"Esploriamo una metodologia di ricerca che enfatizza l'interazione fisica continua con l'ambiente come principale fonte di vincolo per la progettazione di sistemi intelligenti. Mostriamo come questa metodologia abbia recentemente ottenuto successi significativi paragonabili ai più riusciti sforzi classici. Delineiamo possibili lavori futuri in questa direzione che possono portare a sistemi molto più ambiziosi."

Sostanzialmente Brooks sta esplorando un nuovo modo di pensare alla progettazione di sistemi intelligenti, che si concentra sull'interazione fisica con l'ambiente.

Dunque, abbiamo visto che non esiste una definizione universale di intelligenza, lo stesso vale se parliamo di Intelligenza Artificiale poiché gli ambiti di applicazione di quest'ultima sono innumerevoli e in continua evoluzione.[8] All'interno della presente tesi si farà riferimento ad alcune definizioni di IA contenute all'interno dell'ordinamento europeo, ad esempio la definizione data dalla Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e correlati, approvata nel 2018 dalla Commissione europea per l'efficienza della giustizia (CEPEJ): All'interno di questa legge, definita come atto di *soft law*[9], viene descritta l'IA come "insieme di metodi scientifici, teorie e tecniche miranti a riprodurre, tramite macchine, le capacità cognitive degli esseri umani".[10] Un ulteriore definizione per quanto riguarda l'IA è presente nella Comunicazione della Commissione europea del 25 aprile 2018, secondo la quale l'Intelligenza Artificiale ''indica sistemi che mostrano un comportamento

[7] traduzione italiana: "gli elefanti non giocano a scacchi"

[8] A. Santosuosso, *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Mondadori Università, Milano, 2020, 6 ss.; G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo, in Giurisdizione penale: intelligenza artificiale ed etica del giudizio*, Ed. Giuffrè, Milano, 2021, 10.

[9] con atto di *soft law* si intende un atto privo di efficacia vincolante

[10] CEPEJ, *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*, 2018, appendice III, 47. Il documento è consultabile al sito https://rm.coe.int/carta-etica-europeasull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348.

intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi''.[11]

L'IA utilizza enormi quantità di dati (big data) e di informazioni, attraverso un' elaborazione che avviene attraverso algoritmi sofisticati e complessi capaci di estrarre conoscenza dai dati e prendere decisioni che possiamo definire autonome, migliorando costantemente le proprie prestazioni. Attualmente, l'Intelligenza Artificiale si caratterizza come un elemento dirompente, dotata del potenziale di rivoluzionare molteplici ambiti, incluso il mondo giuridico che porta con sé il ruolo determinante di regolare gli aspetti legati all'IA, in particolare sia dal punto di vista tecnico che nelle applicazioni dei sistemi di IA.

Il mondo giuridico inoltre può beneficiare dell'IA anche per una serie di processi in cui le azioni umane possono essere parzialmente sostituite da sistemi intelligenti. L'impiego di sistemi dotati di intelligenza artificiale nel settore della giustizia predittiva o nel settore aziendale ci porta ad osservare scenari nuovi poiché da un lato questi strumenti offrono nuove opportunità, dall'altro lato non sono esenti dal sollevare sfide che necessitano di una sempre maggiore attenzione e di una riflessione dettagliata. Tuttavia, considerando la somiglianza molto marcata con il modo di pensare umano in quanto da esso derivata, l'IA non è intrinsecamente neutrale: spesso i valori e le intenzioni di chi progetta e implementa questi sistemi inevitabilmente influenzano il loro funzionamento, dando alla luce potenziali bias e distorsioni da parte della stessa macchina all'interno del ragionamento.[12]

Per definire tecnicamente e giuridicamente l'Intelligenza Artificiale e per andare ad indagare gli aspetti legati ai sistemi automatici di riconoscimento facciale, è necessaria una premessa utile a delimitare il campo di indagine. Una caratteristica chiave dell'IA è l'Automazione, la quale viene definita come:

"Impiego di un insieme di mezzi e procedimenti tecnici che, agendo opportunamente su particolari congegni o dispositivi, assicurano lo svolgimento automatico di un determinato processo".[13]

---

[11] Commissione europea. (2018, 25 aprile). *L'intelligenza artificiale per l'Europa* (COM(2018) 233 final). https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52018DC0237

[12] S. Signorato, *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, in *Riv. dir. proc.*, 2020, 614.

[13] *https://www.treccani.it/vocabolario/automazione/*

L'automazione dunque è una serie di tecniche che, applicate ad una macchina, consentono di prevedere che questa, a fronte di un input, possa generare una risposta (output). Questo processo ha la particolarità di essere completamente programmato e predeterminato dall'uomo: non è prevista una capacità decisionale o di elaborazione da parte della macchina, la quale deve esclusivamente attenersi alle regole predeterminate fornite per operare. L'automazione è sicuramente fondamentale per il funzionamento dell'AI, ma IA e automazione non devono essere confuse. L'automazione è una tecnica che può avere una serie di input complessi cui fornire output anch'essi da un set complesso: si tratta di tecniche fondamentali che hanno guidato e stanno tuttora avendo un ruolo fondamentale nella rivoluzione tecnologica degli impianti produttivi.[14]

Abbiamo visto come l'automazione serva a far sì che le macchine possano svolgere azioni ripetitive con schemi semplici a partire da set di dati forniti, mentre l'Intelligenza Artificiale presuppone, a differenza della mera automazione, la capacità del sistema di analizzare ed imparare dal proprio ambiente, simulando l'intelligenza umana.

A questo punto è necessario approfondire in che modo l'IA è in grado di imparare autonomamente: il processo che entra in gioco in questo caso prende il nome di *machine learning*, il quale viene definito come un programma che *"apprende dall'esperienza E con riferimento ad alcune classi di compiti T e con misurazione della performance P, se le sue performance nel compito T, come misurato da P, migliorano con l'esperienza E*."[15]

In sostanza, il Machine Learning è una branca dell'Intelligenza Artificiale che si occupa di generare programmi in grado non tanto di svolgere una determinata mansione ma di imparare a svolgere tale mansione.

A questo proposito diventa utile introdurre un ulteriore elemento tecnico che sarà utile a comprendere, nei capitoli successivi, il motivo per cui è così rilevante[16] il tema dell'AI nella giurisprudenza e nell'applicazione commerciale, tenendo conto dell'importanza della tutela dei dati: la rete neurale. Si tratta di un modello computazionale che prevede che le informazioni presenti nell'ambiente (o fornite al sistema) vengano elaborate in maniera distribuita da una moltitudine di unità elementari. Questo aspetto tecnico è particolarmente rilevante perché è in

[14] Shekhar, Sarmah Simanta. "Artificial intelligence in automation." Artificial Intelligence 3085.06 (2019): 14-17.
[15] Mitchell, T. (1997), *Machine Learning*, McGraw Hill. ISBN 0-07-042807-7
[16] Alessandro Mazzetti, Reti neurali artificiali, Apogeo, 1991, ISBN 88-7303-002-5.

grado di portare due fondamentali caratteristiche: resistenza al rumore e resistenza al degrado. La seconda riguarda i sistemi hardware, ossia significa che la Rete neurale è in grado di lavorare anche se il sistema è parzialmente compromesso o difettoso. La resistenza al rumore è invece la caratteristica del sistema di poter operare in presenza di dati incerti, incompleti o leggermente errati.

Sono stati presentati dunque alcuni punti salienti degli aspetti tecnici del funzionamento dei i sistemi automatici basati su Intelligenza Artificiale, non si tratta di una rassegna completa ma di una descrizione funzionale a fornire un quadro sul funzionamento di questi sistemi, che vengono utilizzati, tra le altre, nel campo del diritto.

Per ciò che concerne il sistema giuridico l'IA può offrire diverse opportunità, tra le quali evidenziamo: la capacità di prevedere reati e potenziali autori basandosi su grandi dataset di dati e informazioni, una più rapida semplificazione e risoluzione, attraverso gli algoritmi, di controversie, lo sviluppo di strumenti di analisi volti all'acquisizione di elementi probatori, come ad esempio il riconoscimento facciale automatico. Tuttavia, l'implementazione dell'IA nel sistema giuridico suscita non poche discussioni e disaccordi specialmente inerenti a tematiche legate all'etica e alla protezione dei dati, aprendo anche un dibattito sulla responsabilità di chi, o cosa, commette gli errori e sulla garanzia di mantenere un controllo dell'uomo sulla macchina.[17]

3. IA e privacy

Al fine di affrontare in un modo più consapevole la seconda parte della presente tesi, è utile inoltrarsi prima anche nell'ambito della privacy e dei cambiamenti avvenuti in merito alla sua tutela dopo la comparsa e la diffusione degli strumenti dotati di Intelligenza Artificiale.

Il concetto di privacy nasce come "diritto di essere lasciati soli" e viene ricondotto al famoso *right to privacy* elaborato nel 1890 dalla *Harvard Law Review* grazie al contributo di due giovani giuristi statunitensi: Samuel Warren e Louis Brandeis, i quali teorizzarono il diritto all privacy da intendersi proprio come *right to be let alone*.[18] Tale articolo non chiedeva la mera difesa della solitudine fisica, ma rivendicava la tutela dei valori di autonomia e dignità

[17] 12 F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto Penale e Uomo*, 10/2019, 1, 10.
[18] S. Warren, L. Brandeis, *The right to privacy*, in Harvard Law Review, 5, 1890, 193-220: trad.it. nel vol. *Jus solitudinis*, a cura e con intr. di V. Frosini, Milano 1993 (edizione fuori commercio quale "Strenna natalizia Giuffrè"), 53 ss.

dell'individuo, compresa la protezione della sua cerchia familiare e della cerchia societaria in cui la persona ha scelto di collocarsi.[19] Il right to privacy non trovò subito tutela nelle Corti, ma dovette attendere il 1965 per venire riconosciuto dalla Corte Suprema, la quale elaborò il diritto costituzionale alla privacy, quale fondamento dei diritti di libertà dell'individuo (libertà personale, di manifestazione del pensiero, di comunicazione e così via)[20].

La concezione di privacy si è evoluta, passando da un'ottica passiva, incentrata sul 'diritto a essere lasciati soli', a una prospettiva attiva, focalizzata sul diritto a disporre dei propri dati.

Con l'avvento del digitale, la sfida non è più solo quella di proteggere le informazioni personali, ma anche di controllare come vengono raccolte e utilizzate da terzi.[21] Il diritto alla privacy oggi ha sviluppato una nuova forma, adattandosi alle esigenze di tutela dettate dall'avvento di Internet, dei big data e dell'Intelligenza Artificiale. Alcuni esempi noti di aziende che trattano dati personali degli utenti sono: l'azienda *Amazon* che monitora costantemente le preferenze d'acquisto, *Google* che registra le nostre abitudini quando navighiamo nel web, *Faceebok* conosce le nostre relazioni sociali, e così via.

Tutto questo ha portato ad un ampliamento del concetto di privacy e di conseguenza anche a dei rischi maggiori di violazione della stessa, basti pensare che i nostri dati spesso vengono raccolti a nostra insaputa e talvolta con modalità a cui non conferiamo il giusto peso, come nel caso del riconoscimento facciale.

[19] FROSINI, Tommaso Edoardo. La privacy nell'era dell'intelligenza artificiale. DPCE Online, [S.l.], v. 51, n. 1, apr. 2022. ISSN 2037-6677. Available at: <https://www.dpceonline.it/index.php/dpceonline/article/view/1572>. Date accessed: 23 sep. 2024. doi: http://dx.doi.org/10.57660/dpceonline.2022.1572.

[20] A. Baldassarre, *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974. V. ora la raccolta delle decisioni della Corte Suprema: *The Right to Privacy. Historic US Supreme Court Decisions*, 2012

[21] T.E. Frosini, *Le sfide attuali del diritto ai dati personali*, in S. Faro, T.E. Frosini, G. Peruginelli (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, 2020, 25 ss

Capitolo II: Tecnologie di riconoscimento biometrico

1. Nota introduttiva

All'interno di questo secondo capitolo verrà affrontata una particolare applicazione dell'Intelligenza Artificiale, ossia come essa è in grado di utilizzare il dato biometrico. Questo aspetto è decisivo in quanto è strettamente connesso all'IA che viene utilizzata per lo sviluppo di tecniche di riconoscimento del dato biometrico per molteplici scopi. In particolare, in primo luogo sarà analizzata la definizione e le tipologie di dati biometrici, proseguendo con una disamina di alcuni esempi di utilizzo da parte di aziende private come il *FaceID* da parte di Apple e l'esempio di *worldcoin* sul riconoscimento biometrico dell'iride analizzando le principali controversie normative.

2. Biometria: panorama normativo

Ad oggi l'utilizzo della biometria, in particolare il trattamento del dato biometrico, sia per finalità di interesse pubblico, sia per finalità di interesse privato, rappresenta un ambito molto controverso.

E' necessario in primo luogo individuare quale sia la normativa sulla protezione dei dati personali, tra cui figurano anche quelli biometrici, tenendo conto che è strutturata su più livelli: internazionale, europeo e nazionale.[22]

I primi e più importanti strumenti internazionali per la protezione dei dati personali, adottati dal Consiglio d'Europa sono la c.d. Convenzione 108 del 1989[23], ratificata in Italia con legge 21 febbraio 1989, n. 98, e la seguente Raccomandazione R(87) 15 del Comitato dei Ministri. Questi documenti hanno segnato un punto di svolta nel panorama giuridico internazionale, anticipando molti dei principi poi ripresi dalla normativa europea. Le ragioni che hanno portato alla profonda riforma della normativa europea sulla protezione dei dati hanno spinto, contemporaneamente, il Consiglio d'Europa ad aggiornare la Convenzione 108, adottando il

[22] Mobilio, G. (2021), *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Aracne Editrice.

[23] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale.

Protocollo di Elsinore (c.d. Convenzione 108+), il quale ha introdotto importanti novità, rafforzando la tutela dell'autonomia informativa, del principio di proporzionalità e dei diritti degli interessati.[24]

La Direttiva UE 2016/680 offre una regolamentazione più dettagliata e incentrata nello specifico sul trattamento dei dati biometrici nel contesto delle attività di prevenzione e repressione del crimine, integrando e, in alcuni casi, prevalendo sul Regolamento UE 2016/679 (GDPR), come chiarito dal Considerando n. 34. In base all'art. 10 di tale Direttiva, il trattamento di dati biometrici intesi a identificare in modo univoco una persona fisica è autorizzato solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e in presenza di specifiche condizioni previste dalla Direttiva stessa.

Con il d.lgs. n. 196/2003 il legislatore italiano ha attribuito al Garante privacy il compito di definire delle misure di sicurezza specifiche per il trattamento dei dati biometrici, al fine di garantire la tutela dei diritti degli interessati. Ad ogni modo, l'evoluzione rapida delle tecnologie di riconoscimento facciale, basate sull'intelligenza artificiale, solleva interrogativi sulla capacità del quadro normativo esistente di offrire una protezione adeguata in tutti i casi. L'applicazione di tali sistemi richiede un'interpretazione flessibile delle disposizioni normative e, in alcuni casi, l'adozione di misure di sicurezza supplementari[25].

In Italia con il D.lgs. 51/2018 è stata recepita la direttiva europea sulla protezione dei dati. Il D.lgs. 51/2018 impone una riserva di legge per il trattamento dei dati biometrici, rendendo spesso illegittimo il loro utilizzo in assenza di una specifica disposizione normativa.[26]

Il Garante italiano, all'interno della verifica preliminare n. 155/2018, ha precisato che il riconoscimento facciale configura un trattamento di dati biometrici solo quando il confronto tra l'immagine acquisita e il database avviene in modo automatizzato, tramite software o hardware

---

[24] C. DE TERWANGN, *Council of Europe convention 108 +: A modernised international treaty for the protection of personal data, in International review of law, computers & technology*, 28, 2, 2014.

v. G. GREENLEAF, *Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives, 142 Privacy Laws & Business International Report*, 14-17 agosto 2016; S.L. DUQUE DE CARVALHO, *Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108,* in European data protection law review, 5, 1, 2019, 55 ss.

[25] Art. 2-septies del d.lgs. n. 196/2003

[26] L. SAPONARO, Le nuove frontiere dell'individuazione personale, in Archivio penale – Rivista web, fascicolo n. 1, 2022, (p. 10)

dedicati. In assenza di tale automatizzazione, il trattamento non rientra nell'ambito dei dati biometrici.[27] Tuttavia, qualora il trattamento sia finalizzato a categorizzare le persone in base a caratteristiche fisiche o altre informazioni sensibili, si applicano le norme relative ai dati personali 'particolari', in quanto tali informazioni potrebbero rivelare, ad esempio, l'origine razziale o etnica o le opinioni politiche.[28]

Il quadro normativo italiano sulla protezione dei dati, pur mantenendo alcune specificità nazionali, è stato profondamente riformato dal d.lgs. 101/2018 per allinearsi al GDPR, il regolamento europeo di riferimento in materia, il quale è entrato in vigore nel 2016 ed è stato integrato da altre norme come la direttiva Law Enforcement (c.d.LED)[29].

Il trattamento dei dati biometrici, in particolare quelli ottenuti tramite il riconoscimento facciale, solleva complesse questioni giuridiche. Il Comitato europeo ha precisato che il concetto di 'trattamento di dati biometrici' non si esaurisce nell'identificazione di un soggetto noto. Anche il semplice 'rilevamento' di caratteristiche biometriche al fine della loro successiva conservazione configura un trattamento di dati biometrici, sottoposto alle relative tutele. Il Garante per la privacy italiano ha chiarito che qualora lo scopo del trattamento sia esclusivamente il rilevamento della presenza di un volto all'interno di un'immagine, senza finalità identificative, e senza conservare i dati biometrici acquisiti, non sia da applicare il regime giuridico dei dati biometrici.[30]

Il riconoscimento facciale solleva tuttavia profonde preoccupazioni in merito alla tutela della privacy individuale. Il Regolamento Generale sulla Protezione dei Dati (GDPR) ha introdotto un quadro normativo rigoroso per governare l'utilizzo di tali sistemi, imponendo, tra l'altro,

---

[27] v. ID., *Verifica preliminare*. *Sistema di rilevazione delle immagini dotato di un software che permette il riconoscimento della persona (morfologia del volto)*, n. 155 del 15 marzo 2018, 2.2,

[28] 2 Art. 9, par. 1, del GDPR; art. 10 della LED.;Explanatory Report della Convenzione 108+ (punti 59 ss.).

[29] Ai due atti citati si aggiunge anche il regolamento (UE) 2018/1725, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE

[30] fr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria*, 21 dicembre 2017

l'acquisizione di un consenso esplicito e informato da parte dell'interessato.[31] Tale requisito tuttavia, si rivela particolarmente complesso da soddisfare nel caso dei sistemi di riconoscimento facciale passivi, dove la raccolta dei dati biometrici avviene spesso all'insaputa dell'individuo.

In particolare, il GDPR:

- definisce le regole per il trattamento dei dati personali nell'Unione Europea e assieme alla LED offre strumenti per regolamentarne l'uso. Entrambe le normative, assieme alla Convenzione 108+ hanno introdotto una definizione di "dati biometrici"[32] che include le immagini facciali, qualificandole come dati sensibili il cui trattamento è soggetto a restrizioni.
- bilancia in modo efficace le esigenze della libera circolazione dei dati con la necessità di proteggere la privacy degli individui, offrendo un quadro normativo solido e completo.[33]
- All'interno dell'articolo 4 introduce una definizione specifica per i "dati biometrici" definendoli *"i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici"*.[34] Questi ultimi, a differenza delle semplici immagini, consentono l'identificazione univoca della persona e sono quindi soggetti a restrizioni più severe. Non è sufficiente avere una semplice immagine o un video, per parlare di dato biometrico, ma è necessario che questi dati siano sottoposti a un trattamento tecnico specifico che consenta di estrarre informazioni biometriche utilizzabili per l'identificazione.[35]

[31] GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul consenso ai sensi del regolamento* (UE) 2016/679, 10 aprile 2018, 20

[32] A. IANNUZZI, F. FILOSA, *Il trattamento dei dati genetici e biometrici*, in Dirittifondamentali.it, 2, 2019, 2.

[33] S. SICA, *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Wolters Kluver - Cedam, Milano, 2016, 2

[34] Art.4 GDPR

[35] COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit., 19 s.

- si basa sul principio del consenso informato, limitando severamente il trattamento dei dati biometrici, considerati sensibili, a differenza della LED, la quale, incentrata sulla lotta alla criminalità, autorizza tale trattamento solo in casi eccezionali e ben definiti dalla legge, escludendo il consenso come base giuridica.

Un caso esemplare, a proposito del consenso esplicito,riguarda l'esperienza dell'azienda Facebook che nel 2010 ha introdotto una funzione di riconoscimento facciale automatico, evidenziando le criticità connesse a tali tecnologie. Nonostante l'azienda avesse previsto la possibilità di disattivare la funzione, le autorità garanti della privacy hanno sancito la violazione della normativa vigente, in quanto mancava un consenso esplicito preventivo da parte degli utenti. Tale caso ha sottolineato l'esigenza di un quadro normativo più stringente e di una maggiore consapevolezza da parte dei cittadini sui rischi connessi al trattamento dei dati biometrici, soprattutto quando effettuato in modalità passiva.[36]

Il principio cardine della protezione dei dati personali è la liceità del trattamento. La normativa in materia individua una serie di condizioni che devono essere rispettate affinché un trattamento sia considerato lecito. Nel caso dei sistemi di riconoscimento facciale (TRF), la distinzione tra dati biometrici e non è fondamentale per determinare la liceità del trattamento.

A questo proposito, un ulteriore contributo alla regolamentazione dell'intelligenza artificiale a livello europeo è rappresentato dall' Artificial Intelligence Act (AI Act), approvato dal Parlamento Europeo il 13 marzo 2024 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 12 luglio dello stesso anno. Il Regolamento (UE) 2024/1689 introduce un quadro normativo completo e armonizzato per lo sviluppo e l'utilizzo dei sistemi di intelligenza artificiale all'interno del mercato unico europeo, trattando tra, le altre, anche il tema del riconoscimento facciale.[37]

L'AI Act ha introdotto una vera e propria scala di valutazione del rischio per i sistemi di intelligenza artificiale: a seconda del potenziale impatto negativo sui diritti fondamentali o sulla sicurezza, i sistemi sono classificati in diverse categorie: da quelli a rischio minimo, come i videogiochi, a quelli ad alto rischio, come i sistemi utilizzati per l'assunzione o l'applicazione

[36] Cfr. DATA PROTECTION COMMISSIONER, *Facebook Ireland Ltd. Report of Audit*, 21 dicembre 2011,14. cfr ARTICLE 29 WORKING PARTY, *Opinion 02/2012 on facial recognition in online and mobile services*, WP 192, 22 marzo 2012, p. 4.5.

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

della legge, che sono sottoposti a controlli molto rigorosi. I sistemi che pongono un rischio inaccettabile, ad esempio quelli che manipolano psicologicamente i più vulnerabili, sono addirittura vietati.

Per quanto riguarda il tema del riconoscimento facciale, esso solleva numerose preoccupazioni in termini di privacy, sorveglianza di massa e discriminazione. I sistemi di riconoscimento facciale, in particolare quelli utilizzati in tempo reale in spazi pubblici, sono considerati ad alto rischio secondo la scala di valutazione dell'AI Act. Per questi motivi tale atto normativo cerca di far fronte a tali rischi, stabilendo un quadro normativo rigoroso per l'utilizzo di questa tecnologia e introducendo limiti e divieti come:

- divieto generale dell'utilizzo di sistemi di riconoscimento facciale in tempo reale in spazi accessibili al pubblico, come le strade o le piazze. Questo divieto ha lo scopo di prevenire l'uso indiscriminato di questa tecnologia e mira a proteggere la privacy dei cittadini. Il regolamento prevede alcune eccezioni a questo divieto generale, permettendo l'utilizzo di sistemi di riconoscimento in casi specifici e sotto stretto controllo giudiziario. Ad esempio, è consentito l'utilizzo del riconoscimento facciale in tempo reale per la ricerca di persone scomparse o per prevenire gravi minacce terroristiche.
- divieto di creare banche dati di riconoscimento facciale attraverso l'estrazione indiscriminata di immagini da internet o da filmati di telecamere a circuito chiuso.

Al di fuori degli spazi pubblici, l'utilizzo del riconoscimento facciale è soggetto a requisiti specifici, come la valutazione dell'impatto sulla privacy e la trasparenza nei confronti degli interessati.[38]

Tuttavia, la giurisprudenza in materia è ancora in evoluzione e si prevedono ulteriori sviluppi, soprattutto alla luce delle nuove tecnologie e delle sfide poste dalla crescente digitalizzazione.

[38] M.Borgobello, *Sorveglianza facciale: l'AI Act e il difficile equilibrio tra sicurezza e privacy*, in agendadigitale.eu

3. Il dato biometrico

La compatibilità tra i sistemi che utilizzano la biometria e i diritti fondamentali dei soggetti coinvolti in tale utilizzo è un tema di fondamentale importanza[39]. Per affrontare adeguatamente questo tema è necessario inquadrare ciò che rappresenta la biometria. Questa viene tradizionalmente definita come la «disciplina che studia le grandezze biofisiche allo scopo di identificare i meccanismi di funzionamento, di misurarne il valore e di indurre un comportamento desiderato in specifici sistemi tecnologici».[40] Spesso la biometria viene utilizzata per le attività di identificazione e riconoscimento delle persone, in questi casi si parla di «autenticazione biometrica», ossia di un sistema di identificazione capace di osservare caratteristiche sia «anatomiche o fisiologiche» (ad es. il riconoscimento facciale), sia comportamentali (ad es. il riconoscimento vocale). Il meccanismo alla base del sistema biometrico si articola in due passaggi essenziali:

A) Fase di registrazione del dato biometrico (c.d. *enrollment*): "si procede alla rilevazione e all'acquisizione dell'informazione biometrica sotto forma di dato biometrico grezzo. Quest'ultimo viene poi rappresentato come modello (c.d. *template*), così da potere essere archiviato e confrontato con i dati già acquisiti."[41]

B) Fase di verificazione del template: "questo passaggio si basa sulla comparazione tra i templates già presenti nel sistema e quelli acquisiti istantaneamente a seguito dell'interazione con l'utente. Tale fase è, dunque, finalizzata a verificare la coincidenza o meno tra i dati e, nel caso di esito positivo, il sistema ne decreterà il *matching*."

Occorre precisare che non vi potrà mai esservi piena coincidenza tra i dati, in quanto l'uno e l'altro saranno rappresentati secondo formule matematiche diverse (considerato il differente momento della rilevazione). Per tale ragione, il sistema si basa su risultati di coincidenza approssimativi e fornisce un determinato punteggio, che, a seconda del superamento o meno di

[39] Elettra Currao, *Riconoscimento facciale e diritti fondamentali: quale equilibrio?*, in Diritto Penale e Uomo (DPU), 2021.

[40] Voce "Biometria", in Enciclopedia Treccani online

[41] E. Sacchetto, *Nuove Tecnologie e processo penale*, in Diritto penale contemporaneo, fasc. 2, 2019, pp. 468 ss

una soglia predeterminata di somiglianza, viene registrato come risultato di "*match*" o di "*not match*".

Tra le applicazioni della scienza biometrica in materia di identificazione e autenticazione quello a più noto è l'uso delle impronte digitali, ma è diffuso anche il sistema di riconoscimento biometrico fondato sulla geometria della mano che si basa su forma, grandezza e lunghezza delle dita. Inoltre, sono attualmente in fase di sviluppo sistemi di riconoscimento che si basano sull'iride dell'occhio e sulla retina, anche se molte sono le difficoltà e i *bias* che possono derivare da tale tecnica.[42]

4. Tecnologia *FaceId*

La tecnologia di riconoscimento basata sulle impronte digitali è stata ampiamente superata da uno dei soggetti che maggiormente si trova a dover gestire l'autenticazione con dati biometrici. Si tratta chiaramente di *Apple Inc.* che occupa con i suoi IPhone le prime posizioni nelle classifiche di vendita di smartphone a livello globale.

La tecnologia presente in questi smartphone infatti è passata dal "*Touch ID*" ossia un sistema di riconoscimento, autenticazione ed autorizzazione basato sull'impronta digitale, tramite un sensore apposito inserito nella parte anteriore dello smartphone, ad utilizzare il "*Face ID*" ossia un sistema di riconoscimento che tramite una specifica tipologia di fotocamera denominata "True Depth", acquisisce con precisione i dati del volto che vengono proiettati ed analizzati per creare una mappa di profondità del viso, oltre a catturare un'immagine a infrarossi. Una parte del motore neurale dei chip utilizzati dall'autunno 2017 in poi, trasforma la mappa di profondità e l'immagine a infrarossi in una rappresentazione matematica, che viene confrontata con i dati del volto registrati per consentire l'autenticazione biometrica.[43]

La tecnologia *Face ID* si adatta automaticamente ai cambiamenti minori nell'aspetto degli utenti, come il trucco, un taglio di capelli, ma anche accessori, come cappelli, sciarpe, occhiali

[42] A. Licastro, *Il riconoscimento biometrico alla luce della proposta di Regolamento Europeo sull'Intelligenza Artificiale: rischio "sorveglianza di massa" sventato in parte (per ora*), in diario di di diritto pubblico(2024)

[43] Mainenti, D. A. V. I. D. "*User perceptions of apple's face id.*" Information Science, Human Computer Interaction (DIS805) (2017)

da vista o da sole, e lenti a contatto. Per i modelli usciti dall'autunno 2020, è in grado anche di funzionare se l'utente indossa una mascherina.[44]

Face ID è una tecnologia largamente utilizzata, ma ci sono ulteriori ambiti di ricerca tecnologica per quanto riguarda i dati biometrici in fase di studio e testing. In particolare, uno dei più significativi è sicuramente relativo alla tecnologia di riconoscimento dell'iride.[45]

5. Biometria e scansione dell'iride: l'esempio di *worldcoin*

I sistemi di riconoscimento che si basano sull'iride dell'occhio e sulla retina, non sono esenti da difficoltà e *bias* che possono derivare da tale tecnica, che presenta aspetti ingegneristici ed informatici molto complessi.

In particolare, un caso interessante in questo senso è quello dell'impresa fondata nel 2019 da Alex Blania (CEO) e Sam Altman (Presidente) denominata "*Tools For Humanity*". Ricordiamo che Sam Altman è noto alla cronaca per essere il fondatore di *OpenAI*, la startup che ha lanciato Chat GPT, e dove ora ricopre il ruolo di CEO, una delle IA generative più utilizzate, che ha raggiunto 100 milioni di utenti in 2 mesi, diventando l'applicativo con il tasso di crescita più rapido fino ad ora.[46]

La "*Tools For Humanity*" opera nel settore del riconoscimento dell'iride, in particolare è la società che ha lanciato "*Worldcoin*", una criptovaluta che viene riconosciuta come ricompensa per l'attivazione di un account grazie proprio al riconoscimento dell'iride. L'utilizzo del riconoscimento dell'iride come dato biometrico univoco permetterebbe, secondo gli sviluppatori, di promuovere e tentare di risolvere il tema della "*Proof of Personhood*" ossia la prova di essere un umano.[47] Questo, in possibile sostituzione del processo di KYC ("*Know Your Customer*")[48], come fase di registrazione dell'utente alla piattaforma di worldcoin, potrebbe

[44] Dal sito web Apple: https://support.apple.com/it-it/102381

[45] Registro dei provvedimenti n. 179 del 21 marzo 2024

[46] Milmo, Dan. *"ChatGPT reaches 100 million users two months after launch.*" The Guardian 3 (2023).

[47] Borge, Maria, et al. "*Proof-of-personhood: Redemocratizing permissionless cryptocurrencies*." 2017 IEEE *European Symposium on Security and Privacy Workshops* (EuroS&PW). IEEE, 2017.

[48] con l'espressione *Know Your Customer* si intende un processo di riconoscimento utilizzato dalle aziende per verificare l'identità dei propri clienti e valutare potenziali rischi o intenzioni illegali.

portare ad una rivoluzione notevole nel mondo della finanza, nel settore delle criptovalute. Dal punto di vista tecnico, oltre alla tematica del KYC, la tecnica del "*Proof of Personhood*" ha degli aspetti rilevanti anche nella gestione delle criptovalute nella blockchain. In questo momento infatti, le criptovalute presentano prevalentemente due sistemi di validazione delle transazioni sulla blockchain, ossia il *Proof of Work* (alla base ad esempio di Bitcoin) e *Proof of Stake* (alla base del funzionamento della rete Ethereum). Questi sistemi sono alla base della sicurezza nelle transazioni delle criptovalute, ma presentano dei limiti: *La Proof of Work* per funzionare richiede grandi quantitativi di energia elettrica e potenza di calcolo impiegata, mentre la *Proof of Stake* basando il meccanismo di consenso sulla detenzione di valuta può incorrere in problematiche legate al monopolio, in quanto detenendo grandi quantitativi di una criptovaluta si potrebbe ottenere il consenso ad una transazione in modo sostanzialmente centralizzato.[49] La *Proof of Personhood* invece prevede un sistema in grado di stabilire che un individuo è sia umano che unico. Una volta stabilito questo rapporto, la *Proof of Personhood* dà all'individuo la capacità di affermare di essere una persona reale e diversa da un'altra persona reale, senza dover rivelare la propria identità. Chiaramente, questo sistema potrebbe essere in grado di superare la necessità della *Proof of Work* o della *Proof of Stake* in quanto garantirebbe un sistema di sicurezza basato sulla prova dell'identità, che non comporta le stesse problematiche di consumi energetici o di monopolio. Le ricadute possibili dell'applicazione non si fermano al processo di riconoscimento e verifica dell'utente, e nemmeno al mondo delle criptovalute: la "*Proof of Personhood*" è proposta anche come metodo di autenticazione per sistemi più complessi e delicati come ad esempio quello del voto digitale.[50]

In merito a questo tema dell'identificazione di un individuo, il sistema migliore individuato dalla "*Tools For Humanity*" è quello della scansione e riconoscimento dell'iride. Questo presenta dal punto di vista biometrico degli aspetti migliorativi rispetto al *"Face ID"* e alle impronte digitali. Si tratta di un sistema che garantirebbe di poter affermare che l'utente è unico, umano, e differente da qualsiasi altro umano. La scansione dell'iride è però un dato biometrico di recente discussione.

[49] Platt, Moritz, et al. "T*he energy footprint of blockchain consensus mechanisms beyond proof-of-work.*" 2021 IEEE 21st *International Conference on Software Quality, Reliability and Security Companion* (QRS-C). IEEE, 2021.

[50] Borge, Maria, et al. "*Proof-of-personhood: Redemocratizing permissionless cryptocurrencies.*" 2017 IEEE *European Symposium on Security and Privacy Workshops* (EuroS&PW). IEEE, 2017.

Il riconoscimento biometrico dell'iride presenta problematiche di rilievo, oltre a richiedere una tutela dal punto di vista della gestione della privacy, principale strumento di tutela dei dati biometrici. Da questo punto di vista, in Europa la tematica è emersa in alcuni paesi. Si tratta di:

- Italia: il Garante per la Protezione del Dati Personali, il 02/04/24 ha pubblicato un Comunicato Stampa in cui riassume e spiega il contenuto dell'Avvertimento n. 179 del 21 marzo 2024, ossia che se il progetto Worldcoin, basato sulla scansione dell'iride per verificare l'identità degli utenti approdasse in Italia, con ogni probabilità violerebbe il GDPR, con tutte le conseguenze di carattere sanzionatorio previste dalla normativa.[51]
- Spagna: la Agencia Española de Protección de Datos (AEPD) ha emanato una misura precauzionale che impedisce a Worldcoin di continuare a trattare i dati personali in Spagna. La misura cautelare, prevista dall'articolo 66.1 del GDPR per proteggere i diritti e le libertà degli interessati, è stata approvata dal Tribunale nazionale, il quale ha considerato la salvaguardia dell'interesse generale, che consiste nel diritto alla protezione dei dati personali degli interessati, prevalente rispetto all'interesse particolare di un'azienda. A seguito della misura provvisoria imposta dall'Agenzia, *Tools for Humanity Corporation* ha annunciato modifiche al suo funzionamento, come l'introduzione di controlli per verificare l'età o la possibilità di eliminare il codice dell'iride.[52]
- Portogallo: la *Comissão Nacional de Protecção de Dados* (CNPD) il 26/03/2024 ha sospeso temporaneamente, similmente agli altri due paesi citati, la possibilità di raccogliere i dati biometrici tramite scansione iridea legati a Worldcoin. In particolare, la decisione è stata presa in quanto i dati biometrici raccolti sono regolati dal GDPR, e la raccolta avveniva senza una verifica dell'età dei soggetti, esponendo i minori alla possibilità di cedere i propri dati biometrici in modo non autorizzato.[53]

Chiaramente, anche altri paesi hanno agito in maniera simile, sia in Europa che in altri continenti. Infatti, è bene ricordare che la promessa di denaro virtuale in cambio di una mera

[51] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9999748

[52] https://www.aepd.es/en/press-and-communication/press-releases/worldcoin-commits-to-stop-its-activity-in-spainhttps://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-agencia-ordena-medida-cautelar-que-impide-a-worldcoin-seguir-tratando-datos-personales-en-espana

[53] https://www.cnpd.pt/media/ocrc3lht/news_pt-dpa-suspends-collection-of-biometric-data-by-worldcoin_20240326.pdf

scansione dell'iride può suscitare particolare interesse in paesi a basso reddito, come ad esempio nel caso del Kenya, dove le operazioni di scansione e raccolta dei dati biometrici sono state sospese a causa dell'avvento di migliaia di persone in coda a causa della promessa di ottenimento della valuta virtuale.[54]

L'analisi delle potenziali ricadute legali di Worldcoin richiede un esame attento del quadro normativo nazionale e internazionale. All'interno del nostro ordinamento l'utilizzo dei dati biometrici raccolti da Worldcoin potrebbe configurare la commissione di diversi reati, ad esempio: la raccolta e il trattamento illecito di dati biometrici potrebbero integrare il reato di violazione della riservatezza (art. 615-bis c.p.); se gli utenti di Worldcoin fossero indotti a fornire i propri dati biometrici con false promesse o omettendo informazioni rilevanti, potrebbe configurarsi il reato di truffa (art. 640 c.p.); l''utilizzo della criptovaluta Worldcoin per operazioni di riciclaggio di denaro potrebbe integrare il reato di riciclaggio (art. 648-bis c.p.). Inoltre la violazione delle disposizioni del GDPR può comportare sanzioni amministrative pecuniarie molto elevate e, in alcuni casi, anche responsabilità penali.[55]

Come si evince da quanto esposto, la raccolta di dati biometrici e la gestione della privacy sono temi fondamentali che, legati alle capacità dell'IA in termini di elaborazione, pongono tematiche di regolazione complesse e per le quali ad oggi non sono ancora presenti soluzioni univoche. Una delle soluzioni proposte dalle aziende tech, è quella dell'utilizzo di dati sintetici in alcuni casi in cui è possibile. I dati sintetici hanno la caratteristica di replicare e moltiplicare grazie ad algoritmi di IA i dati reali ottenuti da un campione, e di analizzare trend e andamenti grazie a proiezioni che hanno meno problemi legati alla privacy. Vengono applicati ad esempio in campo sanitario e finanziario.[56]

[54] Dal sito della BBC:https://www.bbc.com/news/world-africa-66383325

[55] Italia. *Codice penale*. Roma: Ministero della Giustizia, 1930.

[56] CARMINE ANDREA. *"L'anonimizzazione è morta? Un'analisi dei dati sintetici come proposta per superare la dicotomia "dato personale-non personale*"." CIBERSPAZIO E DIRITTO 23.71 (2022): 235-259.

Capitolo III: L'utilizzo delle TRF nel settore pubblico e privato

1. Presupposti generali

All'interno di quest'ultimo capitolo verranno analizzati alcuni casi specifici di utilizzo di sistemi basati sull'utilizzo dell'IA, in particolare le tecniche di riconoscimento facciale: in primo luogo verrà esaminato il Sistema Automatico di Riconoscimento Immagini (SARI), in secondo luogo verrà analizzato l'uso delle TRF da parte di grandi aziende private come Amazon e Clearview AI, le quali non prevedono interessi dalle finalità pubbliche, ma utilizzano le TRF per ottenere dei vantaggi prettamente commerciali. Inoltre, verrà approfondito il tema del faceboarding in aeroporto, considerando le recenti esperienze negli aeroporti di Milano-Linate e Catania. Per concludere verrà approfondito il complesso rapporto tra l'utilizzo dei dati biometrici e il diritto penale.

2. TRF e pubblica sicurezza: il sistema SARI

All'interno campo della biometria che comprende varie forme di riconoscimento, le tecnologie di riconoscimento facciale (c.d. TRF) presentano una molteplicità di utilizzi in base ad obiettivi, intensità, incidenza e rischi connessi[57]. Le TRF si basano su procedimenti algoritmici automatizzati complessi, grazie ai quali sono in grado di identificare un individuo a partire dall'immagine del suo volto, confrontandola poi con le immagini precedentemente acquisite e inserite nel database. Appartenendo al vasto ambito delle tecnologie biometriche, i sistemi di riconoscimento facciale sfruttano le caratteristiche uniche del volto umano, tuttavia, la peculiarità delle TRF risiede nella facilità di acquisizione delle immagini, nel costo più contenuto e nella minore invasività rispetto ad altre tecniche biometriche, come il riconoscimento delle impronte digitali o il riconoscimento dell'iride. Quest'ultima caratteristica, la minore invasività, risulta problematica in quanto consente potenzialmente la raccolta di immagini del volto senza il consenso esplicito del soggetto ritratto.

Una interessante applicazione della tecnologia di riconoscimento facciale nel nostro Paese trova attuazione con il Sistema Automatico di Riconoscimento Immagini (SARI), introdotto in Italia

[57] ORLANDO, Alberto. *La regolamentazione delle tecnologie di riconoscimento facciale nell'UE e negli USA: alea IActa est?*. DPCE Online, [S.l.], v. 64, n. 2, july 2024. ISSN 2037-6677.

nel 2017. Tale sistema rappresenta una delle applicazioni più avanzate dell'Intelligenza Artificiale nel campo della sicurezza pubblica. Questa tecnologia, che consente di confrontare immagini di volti catturate da telecamere di sorveglianza con un vasto database di foto segnaletiche, solleva serie preoccupazioni relative alla tutela della privacy e ai diritti civili. L'utilizzo del sistema SARI da parte delle forze dell'ordine ha provocato fin da subito numerosi dubbi. In particolare, è emerso che la banca dati del SARI contiene uno squilibrio significativo tra i volti di individui stranieri rispetto agli italiani, con circa 7 milioni di stranieri su un totale di 10 milioni. Questa disparità è stata giustificata dagli sviluppatori, i quali hanno spiegato che i dati di SARI provengono in gran parte dal precedente sistema, basato sulle impronte digitali, Ssa-Afis.[58]

Il SARI si compone di due moduli principali: SARI *Enterprise* e SARI *Real-Time*. Ognuno di questi moduli presenta caratteristiche e finalità specifiche, inserendosi in un dibattito più ampio sulla tutela della privacy e sull'impatto delle nuove tecnologie sulla società. In Italia il SARI può venire utilizzato solo nella sua funzione *enterprise*, ovvero da remoto[59]. Tale funzionamento consente alle forze dell'ordine di condurre ricerche sui volti altamente efficienti all'interno dell' AFIS-SSA.[60] In meno di 15 secondi, il sistema è in grado di confrontare un'immagine facciale di interesse con un vasto database, generando una lista di possibili corrispondenze (*candidate list*) ordinate per grado di similarità.[61] Questa lista, frutto di un'analisi multilivello che include sia caratteristiche biometriche del volto che dati anagrafici, necessita tuttavia di una verifica finale da parte di un operatore umano esperto in comparazione fisionomica.[62]

---

[58] Elettra Currao, *Riconoscimento facciale e diritti fondamentali: quale equilibrio?*, in Diritto Penale e Uomo (DPU), 2021.

[59]M Colacurci *Riconoscimento facciale **e** rischi per i diritti fondaentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese **e** cittadini*, SISTEMA PENALE, 2022

[60] La banca dati AFIS (Automated Fingerprint Identification System) rappresenta il sistema automatizzato di acquisizione delle impronte digitali, di cui fa parte il Sotto Sistema Anagrafico (Ssa), che contiene, invece, le foto segnaletiche presenti nei database della polizia, insieme alle informazioni fisiche delle persone ritratte.

[61] sito del Ministero dell'Interno, www.interno.gov.it.

v. R. LOPEZ, *La rappresentazione facciale tramite software*, in A. SCALFATI (a cura di), Le indagini atipiche, Giappichelli, Torino, 2019, 239 ss

[62]Cfr. Valeri: 2022.

Nel settembre 2018, SARI *Enterprise* ha dimostrato la sua efficacia sul campo, consentendo l'arresto di due individui di origine georgiana ricercati per un furto. Grazie al riconoscimento facciale, le immagini delle telecamere di sorveglianza sono state confrontate con un vasto database, portando all'identificazione dei responsabili.[63] Poco prima che SARI *Enterprise* dimostrasse tali risultati nell'identificare e arrestare i responsabili di un furto in abitazione, il Garante per la protezione dei dati personali aveva autorizzato l'utilizzo del sistema. All'interno di tale provvedimento il garante ha descritto il sistema SARI *enterprise* come: *"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"*.[64]

SARI *Real-Time* è una tecnologia che, mediante l'analisi biometrica dei volti in tempo reale, consente di confrontare le immagini catturate da sistemi di videosorveglianza con una '*watch-list*' limitata a 10.000 soggetti. L'individuazione di una corrispondenza genera un alert immediato, avvisando i funzionari a cui spetta confermare il riconoscimento.

Per quanto riguarda il panorama italiano, nel marzo 2021 il Garante per la protezione dei dati personali ha espresso un parere negativo sull'utilizzo del sistema SARI *Real Time*, motivando la sua decisione con l'assenza di un'adeguata base giuridica. Tale pronuncia ha evidenziato i potenziali rischi connessi all'impiego del riconoscimento facciale in tempo reale, il Garante ha affermato che tale sistema *real time*: "realizza 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" potendo dare alla luce "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".[65]

---

[63] V., ad es., *Brescia: ladri d'appartamento identificati con il riconoscimento facciale,* 7 settembre 2018, in www.repubblica.it.; *Ecco Sari, il nuovo software di riconoscimento facciale della polizia*, 7 settembre 2018, in www.skytg24.it

[64] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Sistema automatico di ricerca dell'identità di un volto, provvedimento n. 440 del 26 luglio 2018.

[65] Ibidem.e G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 240 ss

L'utilizzo del SARI nel processo penale solleva diverse criticità, infatti è fondamentale garantire che l'utilizzo del SARI sia conforme alla normativa sulla protezione dei dati personali (Reg. UE 2016/679) e che siano adottate misure adeguate per minimizzare i rischi per la privacy.

Uno dei limiti legati all'utilizzo del SARI è che esso potrebbe portare a un'inversione dell'onere della prova, ossia il sospettato si ritrova chiamato a dimostrare la propria innocenza piuttosto che l'accusa a provare la colpevolezza del sospettato.

Inoltre, alcuni studi hanno evidenziato che i sistemi di riconoscimento facciale possono essere soggetti a bias algoritmici, discriminando gruppi di persone sulla base di caratteristiche come il genere, l'etnia o l'età.

Ad oggi Il quadro normativo italiano, in particolare il Codice di Procedura Penale, non contiene disposizioni specifiche sull'utilizzo del SARI. Tuttavia, si applicano le norme generali in materia di prove e di tutela della privacy. La Corte di Cassazione, in alcune pronunce, ha sottolineato l'importanza di una valutazione caso per caso dell'ammissibilità delle prove ottenute attraverso l'utilizzo di sistemi di riconoscimento facciale, tenendo conto dei principi di pertinenza, attendibilità e non contraddittorietà.[66]

3. TRF nell'ambito commerciale

Alla luce degli esempi presentati in precedenza, è possibile affermare che le tecniche di riconoscimento facciale sono parte di una tecnologia in continuo sviluppo, oltre al settore pubblico e della sicurezza esse stanno rivoluzionando anche il modo in cui le aziende interagiscono con i propri clienti.

Vi sono diversi ambiti di applicazione delle TRF nell'ambito commerciale:
Nel settore *retail* i negozi stanno sperimentando l'utilizzo di questa tecnologia per offrire ai clienti un'esperienza sempre più personalizzata. Un esempio è la multinazionale Amazon, la quale ha sperimentato questa tecnologia con la creazione di negozi *AmazonGo* sprovvisti di

[66] Garante per la protezione dei dati personali. (2021). *Parere sul sistema Sari Real Time*.,Colacurci, M. (n.d.). *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini, Proposta di Regolamento della Commissione Europea, IA*. Sistema Penale.

casse, dove i clienti possono prendere gli articoli desiderati e uscire senza dover attendere il loro turno in fila.[67]

All'interno dei negozi *AmazonGo* vi è una complicata rete di sensori, telecamere e algoritmi automatizzati. Una volta che un cliente entra nel negozio, dopo aver scansionato il proprio codice a barre virtuale tramite l'app dedicata, viene monitorato costantemente da un sistema di telecamere che crea una rappresentazione tridimensionale del suo movimento. Ogni prodotto prelevato dallo scaffale viene automaticamente identificato e aggiunto a un carrello virtuale associato al conto del cliente. Una volta terminata la spesa, il cliente può semplicemente uscire dal negozio: l'importo totale degli acquisti verrà addebitato automaticamente sulla sua carta di credito registrata.[68]

Un sistema come *AmazonGo* può sicuramente offrire vari vantaggi ai consumatori come ad esempio la comodità di eliminare la fila in cassa, la velocità di pagamento senza la necessità di manipolare denaro contante o carta di credito, inoltre grazie ai dati raccolti Amazon può offrire esperienze personalizzate in base alle preferenze dei clienti. Ulteriori vantaggi in merito riguardano più in generale il settore *retail*, all'interno del quale grazie a modelli come *AmazonGo* avvengono dei cambiamenti importanti come ad esempio la riduzione dei costi del personale e la riduzione degli sprechi. Tuttavia, sistemi basati sull'utilizzo dell'AI e in particolare del riconoscimento facciale in settori come la vendita, sollevano questioni etiche e sociali poiché la raccolta e l'utilizzo dei dati personali dei clienti possono dar luogo a problematiche legate alla tutela della privacy, l'automazione dei processi potrebbe portare ad una riduzione dell'occupazione nel settore *retail* inoltre un legame di dipendenza da strumenti tecnologici potrebbe portare ad un rischio più elevato di disservizi e attacchi informatici.

Alcune startup come *Grabango* con sede a San Francisco stanno tentando di riprodurre l'approccio di Amazon utilizzando telecamere dotate di intelligenza artificiale per identificare ciò che viene rimosso dagli scaffali per poi addebitare gli articoli nella carta di credito. Ulteriori startup come ad esempio *Caper* e *Veeve* stanno proponendo una strada alternativa, queste aziende hanno integrato telecamere e sensori nei carrelli e utilizzano tecnologie dotate di IA per riconoscere ciò che viene inserito nel carrello: viene integrata una bilancia che pesa gli articoli. I clienti pagano inserendo una carta di credito oppure utilizzando *Apple Pay* o *Google Pay*.

[67] Marco Lorusso, *"Riconoscimento facciale: cos'è e perché trasforma marketing e retail"*, Sergente Lorusso, 12 agosto 2019.

[68] Dal sito della Cnn: https://edition.cnn.com/2019/12/23/tech/smart-shopping-cart/index.html

La diffusione di soluzioni come *AmazonGo* e i carrelli intelligenti solleva importanti questioni etiche e sociali che richiedono un attento bilanciamento tra innovazione e tutela dei diritti individuali.
Le grandi aziende che raccolgono dati sono dunque sempre sotto stretto controllo poiché spesso attività di raccolta dati si trasformano in violazioni della privacy degli individui. Un esempio è lo scandalo connesso alla società americana *Clearview AI*, la quale si è trovata a dover rispondere ad una sanzione del Garante per la privacy a causa delle sue pratiche invasive nel campo del riconoscimento facciale. L'azienda aveva costruito un vasto database contenente miliardi di immagini di volti, raccolte indiscriminatamente da internet. Questo database veniva poi utilizzato per identificare le persone attraverso un sofisticato algoritmo di riconoscimento facciale.

Il problema principale risiede nel fatto che *Clearview AI* ha raccolto e trattato questi dati personali senza il consenso esplicito delle persone interessate, violando così i principi fondamentali del Regolamento generale sulla protezione dei dati (GDPR). Inoltre, l'azienda non ha adottato misure di sicurezza adatte a proteggere i dati sensibili dei suoi utenti.

Di fronte a queste gravi violazioni, il Garante per la protezione dei dati personali italiano ha deciso di intervenire, imponendo a *Clearview AI* una sanzione. Il Garante ha sottolineato come l'attività della società rappresentasse una grave minaccia alla privacy degli individui, in quanto permetteva di monitorare e tracciare i movimenti delle persone senza il loro consenso. Questo caso ha posto l'attenzione sulla necessità di una regolamentazione più stringente del riconoscimento facciale e, più in generale, delle tecnologie di sorveglianza di massa.[69]

4. Faceboarding: sistemi biometrici negli aeroporti

Il *FaceBoarding* è un innovativo sistema di riconoscimento facciale attualmente attivo in Italia negli aeroporti di Milano Linate e Catania, tale tecnologia sviluppata da SEA Milan Airports e da SAC Spa, consente ai passeggeri di accedere ai controlli di sicurezza in aeroporto e di effettuare le procedure di imbarco molto più velocemente dal momento che non diventa più necessario esibire il passaporto, la carta d'identità e la carta d'imbarco, ma è sufficiente

[69] Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022 [9751362], https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751323

mostrare il proprio volto. Il servizio *Face Boarding* è assicurato per i passeggeri di ITA Airways in partenza da Milano Linate e diretto a tutte le destinazioni e a quelli in partenza da Catania e diretti a Milano Linate.[70]

All'interno dell'informativa *privacy-faceboarding* dell'aeroporto di Linate vengono definiti alcuni aspetti fondamentali: innanzitutto il servizio di *faceboarding* può essere utilizzato solamente da soggetti che abbiano compiuto il diciottesimo anno di età e provvisti di carta d'identità elettronica emessa dopo gennaio 2016 o passaporto. La Società per Azioni Esercizi Aeroportuali S.E.A tratta i dati personali dei passeggeri tramite la tecnologia di riconoscimento facciale, in particolare i dati che vengono trattati sono: i dati contenuti nel passaporto o nella carta di identità, i dati biometrici relativi alle caratteristiche del volto e i dati contenuti nella carta di imbarco. All'interno di tale informativa privacy viene puntualizzato che "le immagini relative al volto non saranno conservate nei sistemi aeroportuali, ma utilizzate per creare un modello biometrico".[71]

Il servizio di *Faceboarding* è facoltativo, la base giuridica del trattamento di questi dati personali è il consenso esplicito dell'interessato. Qualora una persona decidesse di negare il consenso ai propri dati personali e di non fornire tali dati, non potrà utilizzare il servizio, ma potrà effettuare le procedure di imbarco secondo i metodi tradizionali. Il servizio di *FaceBoarding* offre due modalità di utilizzo. Se si tratta di un singolo viaggio, è sufficiente registrarsi una volta sola. In alternativa è presente il programma a lungo termine, valido fino al 31 dicembre dell'anno successivo all'iscrizione. In ogni caso, le immagini del volto vengono eliminate subito dopo la creazione del modello biometrico, garantendo la massima sicurezza dei dati personali. A seconda della scelta del programma, i dati personali vengono conservati in due modi diversi: per quanto riguarda il singolo volo se si procede con la registrazione presso il 'chiosco' dell'aeroporto i dati personali vengono automaticamente cancellati dai sistemi aeroportuali dopo 24 ore dalla partenza del volo. Se invece per un singolo volo si sceglie la registrazione tramite App i dati personali vengono eliminati in modo automatico dai sistemi aeroportuali dopo 24 ore dalla partenza del volo, mentre i dati biometrici e i dati contenuti nel documento di identità (c.d. *Digital Travel Credentials*) restano conservati esclusivamente all'interno dello smartphone personale, tramite l'App dedicata, in modo da permettere di associare ulteriori carte d'imbarco senza che si debba ripetere tutta la procedura di registrazione.

[70] https://www.ita-airways.com/it_it/fly-ita/airports/face-boarding.html

[71] informativa privacy-faceboarding: https://www.milanolinate-airport.com/it/voli/face-boarding/privacy

Per ciò che concerne il programma a lungo termine i dati personali vengono eliminati dopo 24 ore dalla partenza del volo, mentre i dati personali relativi al documento di identità e al modello biometrico vengono conservati, protetti da crittografia, fino al 31 dicembre dell'anno in cui aderisce al Programma. Alla fine di tale periodo, tutti i dati personali vengono cancellati in modo irreversibile dai server dell'aeroporto.

In merito al trattamento dei Dati Personali all'interessato viene riconosciuta la facoltà di esercitare i diritti di cui agli articoli da 15 a 22 del Regolamento Generale sulla Protezione dei Dati 2016/679 (GDPR). In particolare, l'interessato ha diritto di ottenere da SEA la rettifica, l'integrazione o la cancellazione (c.d. diritto all'oblio) dei Dati Personali; il diritto di ottenere la limitazione del trattamento e il diritto alla portabilità dei Dati Personali e il diritto di proporre reclamo all'Autorità Garante.Viene inoltre garantito il diritto di revocare il consenso al trattamento (senza che tale revoca pregiudichi la liceità del trattamento effettuato prima della revoca) e di contestare la decisione automatizzata presa da SEA chiedendo l'intervento umano da parte dell'operatore preposto SEA.

In merito al panorama Europeo, il Comitato Europeo per la protezione dei dati (EDPB) ha espresso un parere sull'utilizzo delle tecnologie di riconoscimento facciale da parte degli operatori aeroportuali e delle compagnie aeree, in particolare il presidente dell'EDPB Anu Talus ha affermato le seguenti parole: "Sempre più operatori aeroportuali e compagnie aeree di tutto il mondo stanno sperimentando sistemi di riconoscimento facciale che consentono ai passeggeri di passare più facilmente attraverso i vari punti di controllo. È importante essere consapevoli del fatto che i dati biometrici sono particolarmente sensibili e che il loro trattamento può creare rischi significativi per le persone. La tecnologia di riconoscimento facciale può portare a falsi negativi, pregiudizi e discriminazioni. L'uso improprio dei dati biometrici può anche avere gravi conseguenze, come la frode di identità o l'impersonificazione. Pertanto, esortiamo le compagnie aeree e gli operatori aeroportuali a optare per modi meno intrusivi per semplificare i flussi di passeggeri, quando possibile. Secondo l'EDPB, le persone fisiche dovrebbero avere il massimo controllo sui propri dati biometrici."[72]

L'obbligo di verificare l'identità dei passeggeri aerei con un documento d'identità varia a seconda del paese membro dell'UE. Per questo motivo l'utilizzo di dati biometrici con questo

[72]EuropeanDataProtectionBoard,https://www.edpb.europa.eu/news/news/2024/facial-recognition-airports-individuals-should-have-maximum-control-over-biometric_it

scopo dovrebbe essere proporzionato alla necessità effettiva di tale verifica e limitato ai casi in cui essa sia legalmente richiesta.
L'EDPB ha analizzato diverse potenziali modalità di conservazione dei dati biometrici e ha concluso che solo quelle che prevedono la conservazione dei dati direttamente da parte dell'individuo o in una banca dati centrale accessibile solo con una chiave crittografica personale offrono garanzie sufficienti in termini di privacy e sicurezza. Per quanto riguarda la durata della conservazione, questa deve essere limitata al tempo strettamente necessario e adeguatamente giustificata.
Al momento, il Face Boarding è una tecnologia relativamente nuova nel settore aeroportuale europeo, e la sua diffusione è ancora limitata a pochi ambienti, quali Milano Linate e Catania.. Tuttavia, questa tecnologia si sta ampliando gradualmente grazie ai suoi vantaggi in termini di efficienza e sicurezza.

5. L'uso del dato biometrico all'interno del processo penale

Il dato biometrico, frutto dell'elaborazione automatica, costituisce una prova digitale nel processo penale.[73] Esso, in quanto informazione con valore probatorio in formato digitale[74], richiede specifiche competenze tecniche per la sua raccolta. Tuttavia, la principale criticità legata all'utilizzo del dato biometrico nel processo penale risiede nell'assenza di una disciplina normativa esaustiva.[75] Questa lacuna normativa, aggravata dall'introduzione del D.lgs. 51/2018, che impone una riserva di legge per il trattamento dei dati biometrici, rende spesso illegittimo il loro utilizzo in assenza di una specifica previsione di legge[76].

Nonostante l'importanza crescente del dato biometrico, il nostro ordinamento non dispone di una disciplina specifica che ne regoli l'utilizzo nel processo penale. Questa lacuna normativa rende difficile inquadrare il dato biometrico all'interno delle categorie tradizionali di prove. Il Codice di procedura penale (c.p.p.), da parte sua, disciplina le modalità di acquisizione e utilizzo delle prove. L'articolo 234 c.p.p. ammette l'acquisizione di documenti che

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

rappresentano fatti, persone o cose mediante la fotografia o qualsiasi altro mezzo.[77] Tuttavia, l'applicazione di questa norma al riconoscimento facciale non è del tutto pacifica, in quanto la natura automatizzata e intrusiva di questa tecnologia solleva dubbi sulla sua compatibilità con i principi costituzionali. Sebbene si sia tentato di ricondurre il riconoscimento facciale alle figure della ricognizione fotografica e dell'identificazione (art.349 c.p.p.), queste soluzioni presentano limiti significativi. Il vuoto normativo specifico ai dati biometrici e la natura automatizzata del processo rendono difficile una loro diretta applicazione. La sottoposizione al riconoscimento facciale, soprattutto in assenza del consenso dell'interessato, potrebbe violare il diritto a non autoincriminarsi e la libertà morale.[78]Quest'ultima, intesa come forma di autodeterminazione nelle proprie scelte difensive, viene inevitabilmente compromessa quando l'autorità procede all'identificazione in modo coattivo.

Un'altra ipotesi interpretativa è quella di considerare il dato biometrico facciale alla stregua di una prova documentale.[79] Tuttavia, questa soluzione non è priva di criticità, in quanto non tiene conto della specificità di questa tecnologia e delle sue potenziali implicazioni per la privacy.

Alla luce delle criticità sopra esposte, appare evidente la necessità di una regolamentazione specifica per il dato biometrico nel processo penale. Tale regolamentazione dovrebbe definire le condizioni di ammissibilità e utilizzo di questa tecnologia, garantendo nel contempo la tutela dei diritti fondamentali e l'affidabilità dei risultati.[80]

[77] Dispositivo dell'art. 213 c.p.p.

[78] G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, in Ricerche giuridiche n. 224, 2021, (p. 87, 88)

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

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

CONCLUSIONI

Alla luce di quanto emerso dall'analisi svolta in questa tesi, è possibile dare una risposta al quesito posto nell'introduzione in merito all'utilizzo nel processo penale delle prove ottenute grazie a sistemi di riconoscimento biometrico coadiuvati dall'IA.

E' stato evidenziato grazie ai vari esempi riportati che i sistemi di riconoscimento facciale esistenti non offrono ancora garanzie sufficienti in termini di affidabilità e scientificità. La comunità scientifica non ha raggiunto un consenso unanime sulla loro validità, e i margini di errore sono ancora troppo elevati. Inoltre, la mancanza di trasparenza sui metodi utilizzati e la resistenza dei produttori a rendere pubblici i dati limitano ulteriormente la fiducia in queste tecnologie.

Per quanto riguarda l'Italia, la normativa vigente non offre ancora un quadro completo e specifico per regolamentare l'utilizzo dei dati biometrici, raccolti ed eventualmente elaborati anche grazie a sistemi di IA, come ad esempio il riconoscimento facciale. Le disposizioni generali citate all'interno della presente tesi, richiamate dal Garante, risultano utili come riferimento ma non sono al momento sufficienti a coprire tutti i possibili casi d'uso di questa tecnologia.

Nel nostro ordinamento è previsto il principio di *extrema ratio*, il quale impone che il riconoscimento facciale sia utilizzato solo nei casi in cui sia l'unica soluzione possibile per tutelare un interesse pubblico particolarmente rilevante. Limitando l'applicazione di queste tecnologie ai soli reati più gravi, si garantisce che l'intrusione nella sfera privata sia proporzionata al fine perseguito. Inoltre, la definizione di criteri oggettivi e misurabili per l'utilizzo di tali strumenti contribuisce a rendere più trasparente e controllabile il loro impiego, rafforzando la fiducia dei cittadini nelle istituzioni.

Analizzando il caso inerente alla cryptovaluta *worldcoin*, si è visto come la raccolta e il trattamento illecito di dati biometrici potrebbero integrare alcune fattispecie di reato previste dal codice penale.

Nonostante queste limitazioni, il riconoscimento facciale può essere utile nella fase investigativa, fornendo indizi preziosi per indirizzare le indagini. Tuttavia, l'utilizzo di questi strumenti richiede l'adozione di precise garanzie procedurali per tutelare i diritti dei sospettati.

Il principio di bilanciamento dei diritti fondamentali, pur necessario per la convivenza civile, deve essere condotto con cautela. La compressione di un diritto è ammissibile solo se proporzionata, necessaria e ultima ratio. Tuttavia, il diritto alla dignità umana, in quanto fondamento dell'ordinamento giuridico, non può essere oggetto di bilanciamento. Pertanto, qualsiasi misura che possa ledere la dignità umana, come l'utilizzo indiscriminato del riconoscimento facciale, è in contrasto con i principi costituzionali.

In conclusione, sulla base di tutte le ragioni sopra citate, la risposta al quesito: "la prova ottenuta mediante riconoscimento facciale può essere utilizzata in un processo penale?" Al momento non può che essere negativa, ma è sicuramente un ambito di interesse che merita ulteriori approfondimenti che seguano e analizzino tutte le evoluzioni tecnologiche e giuridiche in merito.

BIBLIOGRAFIA

R. L. Gregory, «*Intelligence*», in *The Oxford Companion to the Mind*, a cura di R. L. Gregory, Oxford University Press, 1987, p. 375-379, p. 375.

Sartor, G. (2022). *L'intelligenza artificiale e il diritto* (1a ed.). Giappichelli

a proposal for the dartmouth summer research project on artificial intelligence di J.McCarthy

R.C. Schank, What's IA, Anyway?, in IA Magazine, Winter 8(4), 1987, pp. 59 ss.

Sartor, G. (2022). *L'intelligenza artificiale e il diritto* (1a ed.). Giappichelli.

A.Santosuosso, *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Mondadori Università, Milano, 2020, 6 ss.;

G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo, in Giurisdizione penale: intelligenza artificiale ed etica del giudizio*, Ed. Giuffrè, Milano, 2021, 10.

CEPEJ, *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*, 2018, appendice III, 47.

Commissione europea. (2018, 25 aprile). *L'intelligenza artificiale per l'Europa* (COM(2018) 233 final).

S. Signorato, *Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo*, in *Riv. dir. proc.*, 2020, 614.

Shekhar, Sarmah Simanta. "Artificial intelligence in automation." Artificial Intelligence 3085.06 (2019): 14-17

Mitchell, T. (1997), *Machine Learning*, McGraw Hill. ISBN 0-07-042807-7

Alessandro Mazzetti, Reti neurali artificiali, Apogeo, 1991, ISBN 88-7303-002-5

12 F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto Penale e Uomo*, 10/2019, 1, 10.

S. Warren, L. Brandeis, *The right to privacy*, in Harvard Law Review, 5, 1890, 193-220: trad.it. nel vol. *Jus solitudinis*, a cura e con intr. di V. Frosini, Milano 1993 (edizione fuori commercio quale “Strenna natalizia Giuffrè”), 53 ss.

FROSINI, Tommaso Edoardo. La privacy nell’era dell’intelligenza artificiale. DPCE Online, [S.l.], v. 51, n. 1, apr. 2022. ISSN 2037-6677.

A.Baldassarre, *Privacy e Costituzione. L’esperienza statunitense*, Roma, 1974. V. ora la raccolta delle decisioni della Corte Suprema: *The Right to Privacy. Historic US Supreme Court Decisions*, 2012

T.E. Frosini, *Le sfide attuali del diritto ai dati personali*, in S. Faro, T.E. Frosini, G. Peruginelli (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, 2020, 25 ss

Elettra Currao, *Riconoscimento facciale e diritti fondamentali: quale equilibrio?*, in Diritto Penale e Uomo (DPU), 2021.

E. Sacchetto, *Nuove Tecnologie e processo penale*, in Diritto penale contemporaneo, fasc. 2, 2019, pp. 468 ss.

Mainenti, D. A. V. I. D. "*User perceptions of apple’s face id.*" Information Science, Human Computer Interaction (DIS805) (2017)

Registro dei provvedimenti n. 179 del 21 marzo 2024

Milmo, Dan. *"ChatGPT reaches 100 million users two months after launch.*" The Guardian 3 (2023).

Borge, Maria, et al. "*Proof-of-personhood: Redemocratizing permissionless cryptocurrencies*." 2017 IEEE *European Symposium on Security and Privacy Workshops* (EuroS&PW). IEEE, 2017.

Platt, Moritz, et al. "T*he energy footprint of blockchain consensus mechanisms beyond proof-of-work.*" 2021 IEEE 21st *International Conference on Software Quality, Reliability and Security Companion* (QRS-C). IEEE, 2021.

Borge, Maria, et al. "*Proof-of-personhood: Redemocratizing permissionless cryptocurrencies.*" 2017 IEEE *European Symposium on Security and Privacy Workshops* (EuroS&PW). IEEE, 2017.

CARMINE ANDREA. *"L'anonimizzazione è morta? Un'analisi dei dati sintetici come proposta per superare la dicotomia "dato personale-non personale*"." CIBERSPAZIO E DIRITTO 23.71 (2022): 235-259.

ORLANDO, Alberto. *La regolamentazione delle tecnologie di riconoscimento facciale nell'UE e negli USA: alea IActa est?*. DPCE Online, [S.l.], v. 64, n. 2, july 2024. ISSN 2037-6677.

Mobilio, G. (2021), *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Aracne Editrice.

C. DE TERWANGN, *Council of Europe convention 108 +: A modernised international treaty for the protection of personal data, in International review of law, computers & technology*, 28, 2, 2014.

G. GREENLEAF, *Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives, 142 Privacy Laws & Business International Report*, 14-17 agosto 2016;

S.L. DUQUE DE CARVALHO, *Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108, in European data protection law review, 5, 1, 2019, 55 ss.*

A. IANNUZZI, F. FILOSA, *Il trattamento dei dati genetici e biometrici*, in Dirittifondamentali.it, 2, 2019, 2.

S. SICA, *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Wolters Kluver - Cedam, Milano, 2016, 2

Art.4 GDPR

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, cit., 19 s.

fr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria*, 21 dicembre 2017

2 Art. 9, par. 1, del GDPR; art. 10 della LED. Explanatory Report della Convenzione 108+ (punti 59 ss.).

Art. 2-septies del d.lgs. n. 196/2003

GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul consenso ai sensi del regolamento* (UE) 2016/679, 10 aprile 2018, 20

DATA PROTECTION COMMISSIONER, *Facebook Ireland Ltd. Report of Audit*, 21 dicembre 2011,14. cfr ARTICLE 29 WORKING PARTY, *Opinion 02/2012 on facial recognition in online and mobile services*, WP 192, 22 marzo 2012, p. 4.5.

M Colacurci *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, SISTEMA PENALE, 2022

v. R. LOPEZ, *La rappresentazione facciale tramite software*, in A. SCALFATI (a cura di), Le indagini atipiche, Giappichelli, Torino, 2019, 239 ss

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell'identità di un volto*, provvedimento n. 440 del 26 luglio 2018.

G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 240 ss

Marco Lorusso, *"Riconoscimento facciale: cos'è e perché trasforma marketing e retail"*, Sergente Lorusso, 12 agosto 2019.

G. Silvestri, L'individuazione dei diritti della persona, in Diritto penale contemporaneo, 29 ottobre 2018, p. 11.

Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024

M.Borgobello, *Sorveglianza facciale: l'AI Act e il difficile equilibrio tra sicurezza e privacy*, in agendadigitale.eu

Italia. *Codice penale*. Roma: Ministero della Giustizia, 1930.

A.Licastro, *Il riconoscimento biometrico alla luce della proposta di Regolamento Europeo sull'Intelligenza Artificiale: rischio "sorveglianza di massa" sventato in parte (per ora*), in diario di di diritto pubblico(2024)

L. SAPONARO, Le nuove frontiere dell'individuazione personale, in Archivio penale – Rivista web, fascicolo n. 1, 2022, (p. 10)

R.V.O. Valli, Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini, in Il Penalista, 16 gennaio 2019.

L. Luparia Donati, Privacy, diritti della persona e processo penale, in Dir. Pen. Proc., 2019, fasc. 6, pp. 1448 ss.

SITOGRAFIA

https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52018DC0237

https://www.treccani.it/vocabolario/automazione/

https://support.apple.com/it-it/102381

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9999748

https://www.aepd.es/en/press-and-communication/press-releases/worldcoin-commits-to-stop-its-activity-in-spain

https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-agencia-ordena-medida-cautelar-que-impide-a-worldcoin-seguir-tratando-datos-personales-en-espana

https://www.cnpd.pt/media/ocrc3lht/news_pt-dpa-suspends-collection-of-biometric-data-by-worldcoin_20240326.pdf

https://www.bbc.com/news/world-africa-66383325

www.interno.gov.it.

https://edition.cnn.com/2019/12/23/tech/smart-shopping-cart/index.html

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751323

https://www.milanolinate-airport.com/it/voli/face-boarding/privacy

https://www.ita-airways.com/it_it/fly-ita/airports/face-boarding.html

https://www.edpb.europa.eu/news/news/2024/facial-recognition-airports-individuals-should-have-maximum-control-over-biometric_it

RINGRAZIAMENTI

Giunta alle conclusioni di questo elaborato ritengo doveroso ringraziare il Prof.Massimo Bolognari per la disponibilità e la pazienza, per avermi assistita nella stesura della tesi e per aver accolto le mie proposte.

Un ringraziamento fondamentale va ai miei genitori, coloro che oltre alla loro fiducia e al loro supporto mi hanno dato la possibilità di studiare ciò che mi piace, voglio esprimere la mia riconoscenza a loro per aver creduto in me anche quando io non ci credevo.

Ci tengo a ringraziare mio fratello Thomas, il quale mi ha sempre fornito ottimi consigli di vita e mi è sempre stato vicino guardandomi sempre con occhi fieri.

Mi preme ringraziare Nicolò per il suo prezioso aiuto e i suoi preziosi consigli, per essere stato partecipe in tutti i momenti belli e non di questi anni così importanti per me.

Ovviamente, un grazie va alle mie amiche più care, Gloria, Elena, Anna, la vostra amicizia è rara e preziosa, ho sempre contato su di voi e continuerò a farlo.

Un ringraziamento a tutte le '*mishe'*, agli amici, ai compagni di università e di avventure, con voi tutti ho vissuto momenti indimenticabili.

Infine ci tengo a dedicare un ringraziamento ai nonni, in particolare a Nonno Giovanni, so quanto sarebbe orgoglioso.