UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Diritto Privato e Critica del Diritto

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea Magistrale in

Giurisprudenza

LA TUTELA DELLO SPAZIO PUBBLICO NEI CONFRONTI DEL RICONOSCIMENTO FACCIALE: USA E UE A CONFRONTO

RELATORE: PROF. ANDREA PIN

STUDENTE: VERONICA MENEGHETTI

ANNO ACCADEMICO 2020/2021

INDICE

INTRODUZIONE

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say".[1]

L'elaborato mira ad affrontare il tema del riconoscimento facciale, in relazione alle implicazioni giuridiche che il suo impiego ha sulla privacy delle persone negli spazi pubblici. Si tratta di una tecnologia recente e in costante evoluzione, che manca di un quadro normativo che regoli il suo utilizzo e le conseguenze che questo comporta. Inoltre, il software in questione vede il cimentarsi dei grandi produttori del settore dell'Information Technology (IT) nella creazione di software di identificazione biometrica sempre più performanti e dunque invasivi della vita delle persone.

L'interesse per la materia è sorto a seguito della trattazione del tema nel corso di Diritto pubblico comparato e della conseguente possibilità offertami di partecipare ad un webinar nel marzo 2021, in cui uno dei relatori, il professor Woodrow Hartzog, esperto di legge e computer science alla Northeastern University, ha affrontato il problema del facial recognition, quale strumento di sorveglianza che permea la sfera personale di ciascuno. Le sue potenzialità quale strumento di oppressione e la mancanza di una regolamentazione chiara e specifica, mi hanno spinto ad approfondire tale questione, con l'obbiettivo di indagare quali siano gli attuali strumenti normativi impiegati nella disciplina della tecnologia, sempre più diffusa (basti pensare al sistema di sblocco degli smartphone o dei pc che sfrutta il sistema di riconoscimento facciale), nei due sistemi giuridici occidentali più vicini a noi: l'Unione Europea e gli Stati Uniti d'America. Si è trattato dunque di elaborare un confronto tra due strutture democratiche che condividono molti dei principi giuridici posti alla base dei rispettivi ordinamenti e analizzare le ripercussioni che l'impiego delle tecnologie di riconoscimento facciale (TRF) da parte delle pubbliche autorità ha nella privacy delle persone.

[1] «Edward Snowden Compares Privacy to Freedom of Speech», University of Arizona News, 28 marzo 2016, https://news.arizona.edu/story/edward-snowden-compares-privacy-freedom-speech.

Nell'analizzare le diverse implicazioni giuridiche mi sono imbattuta nel tema del consenso che potrebbe sembrare centrale in un primo momento. Tuttavia, le coordinate lungo le quali si svolge il riconoscimento facciale negli spazi pubblici sono tali per cui questo non sia utilizzabile: da un lato sarebbe impossibile chiedere a ciascuno il consenso ogni qualvolta si installi una telecamera in un luogo e dall'altra esistono interessi, come la sicurezza nazionale, che sono in grado di derogare a tale esigenza. Ciò rende la tematica del facial recognition peculiare rispetto al dibattito generale sulla privacy.

Pertanto, ho deciso di strutturare la tesi partendo da una breve introduzione relativa al concetto di privacy, delineandone le origini e la sua rilevanza negli spazi pubblici, al fine di comprendere della necessità di un suo ripensamento a causa della diffusione delle nuove tecnologie e in modo particolare delle TRF. Nel secondo capitolo ho introdotto il tema del riconoscimento facciale, analizzando il suo funzionamento, le implicazioni giuridiche che l'artificial intelligence (AI) comporta e le ripercussioni che le TRF hanno per quei diritti fondamentali riconosciuti e sanciti nelle carte costituzionali e internazionali. Successivamente ho proseguito con la comparazione delle legislazioni vigenti nei due sistemi giuridici presi in esame: il terzo capitolo tratta della regolamentazione nell'Unione Europea, analizzando gli utilizzi della tecnologia in questione dalle diverse autorità e dei diversi stati e delineando l'approccio europeo in relazione all'AI, anche alla luce della proposta di regolamento presentata nell'aprile 2021; l'ultimo capitolo affronta la disciplina normativa presente negli Stati Uniti, che la rende peculiare per l'eterogeneità della regolamentazione nei diversi paesi e per l'uso massivo che le forze dell'ordine ne hanno fatto negli ultimi anni.

L'elaborato, dunque, pone l'attenzione su come le normative vigenti appaiano non idonee a contenere tale tecnologia ampiamente innovativa e utile, ma altamente invasiva della privacy di ciascuno.

1. SPAZIO PUBBLICO

1.1 Come nasce il concetto di privacy

Il concetto moderno di privacy risale al 1890, quando due giuristi statunitensi, Samuel Warren e Louis Brandeis, scrivono su Harvard Law Review l'articolo "The Right to Privacy", nel quale individuano come necessaria una regolamentazione di quello che il giudice Cooley definiva "the Right to be let alone". Due anni prima il giudice Cooley, in una pronuncia sugli illeciti extracontrattuali, dunque in ambito diverso rispetto a quello trattato dai due giuristi, aveva delineato "the Right to be let alone". Era fondamentale l'intervento dei tribunali, al fine di proteggere l'individuo dall'intrusione che si stava perpetrando in "the sacred precincts of private and domestic life" da parte di giornalisti, reso possibile dallo sviluppo della fotografia istantanea e del relativo inserimento nei quotidiani.[2] Il diritto alla privacy nasce dunque con un'accezione individualistica e correlata al diritto di proprietà. Si tratta di un diritto a contenuto negativo: il soggetto deve poter mantenere la riservatezza su determinate questioni di natura personale.

In tale contesto si inserisce, circa quarant'anni dopo, anche l'opinione dissenziente di L. Brandeis, divenuto giudice alla Supreme Court, che nella sentenza *Olmestead v. United States*, riguardante un caso di intercettazioni telefoniche, scrive che il governo ha conferito alle persone il diritto di essere lasciati soli.[3]

Una successiva evoluzione della nozione, che emerge in alcune sentenze degli Stati Uniti, considera la privacy anche come protezione dall'ingerenza dei pubblici poteri: gli storici casi *Griswold v. Connecticut*[4] e *Roe v. Wade*[5] sanciscono che esiste uno spazio che deve essere sottratto all'intervento da parte del legislatore. La privacy del soggetto deve essere rispettata affinché possa essere garantita la sua libertà[6].

---

[2] Warren e Brandeis, «The Right to Privacy», *Harvard Law Review* 4, n. 5 (1890): 193–220, https://doi.org/10.2307/1321160.

[3] «Olmstead v. United States, 277 U.S. 438 (1928) », Justia Law, consultato 26 ottobre 2021, https://supreme.justia.com/cases/federal/us/277/438/.

[4] Griswold v. Connecticut, 381 U.S. 479 (1965).

[5] Roe v. Wade, 410 U.S. 113 (1973).

[6] Paolo Patrono, «Privacy e vita privata», in *Diritto penale* (De Giuffrè).

Tale concetto, seppur teorizzato per la prima volta dai due avvocati di Boston, era già noto in Europa a metà Ottocento, ma ciò che distingueva i due continenti, era il fatto che il rispetto della vita privata veniva connesso alla dignità dell'individuo: si volevano garantire a tutti i cittadini gli stessi diritti, cercando di attribuire i privilegi dei più ricchi anche ai meno abbienti, sulla base di principi quali l'eguaglianza, l'autodeterminazione e il rispetto della libertà.[78]

La prima codificazione del diritto alla privacy si ebbe, a livello internazionale, nella Dichiarazione universale dei diritti umani del 1948, il cui l'art. 12 sancisce "Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni". Tale principio è stato recepito poi nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950 all'art.8 e nel Patto internazionale sui diritti civili e politici del 1966 all'art.17.[9]

Con la diffusione delle tecnologie e ancor di più con l'avvento di Internet, i problemi relativi al diritto alla privacy si sono focalizzati sull'esigenza di tutelare i dati personali onde evitare che questi vengano divulgati o dati a terzi al fine di discriminare il soggetto[10]. Ciò che ne consegue è la nascita di un nuovo diritto, simile, ma con delle differenze: si tratta del diritto alla protezione dei dati personali. Nato nell'era della diffusione dei sistemi di informatizzazione, esso si caratterizza per un contenuto a carattere positivo: il soggetto deve poter controllare l'utilizzo delle

[7] Giovanni Sartor e Mario Viola De Azevedo Cunha, «Il caso Google e i rapporti regolari USA/EU», *Diritto dell'Informazione e dell'Informatica (Il)*, n. 4–5 (2014): 657–66, https://bibliotecariviste.giuffrefrancislefebvre.it/#/details?id_doc_master=4402550&fromSearch=&fromFilters=true.

[8] Sergio Niger, «Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali / Sergio Niger», <<Le >>monografie di Contratto e impresa (Padova: CEDAM, 2006).

[9] Alessandro Stiano, «Il diritto alla privacy alla prova della sorveglianza di massa e dell'intelligence sharing: la prospettiva della corte europea dei diritti dell'uomo», *Rivista di diritto internazionale*, n. 2 (2020): 511–18, blob:https://dejure.it/5c4aa259-a437-4844-b1e1-442433c71647.

[10] Tommaso Edoardo Frosini, «Il costituzionalismo nella società tecnologica», *Diritto dell'Informazione e dell'Informatica (Il)*, n. 3 (2020): 471–74, blob:https://dejure.it/195053d3-322a-4ec8-8b6b-edda586622e0.

proprie informazioni personali, anche se pubbliche o comunque non strettamente riservate.[11]

Dalla prima teorizzazione fino ad oggi si è assistito alla produzione di una pluralità di norme giuridiche che regolano la privacy, ma ciò che emerge è la mancanza di coesione.

Nonostante l'evoluzione storica del concetto di privacy, il reale significato di privacy è ancora controverso. Ognuno di noi sa cosa si intende quando ci si riferisce al concetto di privacy, però nel momento in cui ci si trova a doverlo definire, si è disorientati. Lo si associa molto spesso a concetti quali il controllo, la segretezza, "the right to be let alone", però ognuna di questa nozione è poco adatta a descrivere cosa effettivamente sia.[12] Arthur Miller in merito alla definizione del concetto di privacy affermava che fosse "exasperatingly vague and evanescent".[13] La difficoltà nel trovare un giusto significato del termine privacy emerge ancor di più quando questa si trova a dover essere bilanciata con altri valori, quali la sicurezza nazionale, l'imprenditorialità o l'efficienza, oppure si vada a scontrare con altri fattori quali lo sviluppo tecnologico, passando in secondo piano per non essere considerata in opposizione al processo.

Alla luce di tale complessità, come scrive Julie Cohen in *What is privacy*, ciò che risulta fondamentale per delineare il concetto di privacy è considerare che il soggetto si trova inserito nella società, dove instaura costantemente relazioni con gli altri, svolge pratiche e credenze, che non permettono di inquadrarlo, alla luce delle teorie classiche della privacy, in una condizione fissa, con un nucleo autonomo, ma piuttosto in contesti sociali e culturali dinamici.[14] Per questo il significato di privacy non corrisponde alla storica definizione delineata da Warren e Brandeis, in quanto troppo ristretta, né può essere associata a nozioni quali il controllo, dal momento che non risulta necessario né sufficiente e non spiega il criterio secondo cui alcuni dati debbano essere considerati privati e altri no. La nozione risulta più ampia di un diritto

[11] Agenzia dell'Unione europea per i diritti fondamentali, *Manuale sul diritto europeo in materia di protezione dei dati* (Lussemburgo, 2018), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9113547.

[12] Woodrow Hartzog, «Privacy'S Blueprint: The Battle to Control the Design of New Technologies / Woodrow Hartzog» (Cambridge (Massachusetts) London (England): Cambridge Massachusetts: London England, 2018).

[13] Charles R. Ashman, «The Assault on Privacy by Arthur R. Miller», *DePaul Review* 20, n. 10 (1971), https://via.library.depaul.edu/law-review/vol20/iss4/10.

[14] Julie E. Cohen, «What Is Privacy», *Harvard Law Review* 126, n. 7 (2013): 1904–33.

individuale.[15] Secondo Helen Nissenbaum la privacy deve essere intesa come integrità contestuale: la violazione della privacy sussiste nel momento in cui si verifica la diffusione di un'informazione personale, non rispettando il contesto in cui è stata condivisa. Per Daniel Solove invece, l'errore nella concettualizzazione della privacy consta nel fatto che non la si consideri a gradi: è necessario allontanarsi dall'idea di privacy come segretezza assoluta e valutare come esistano dati che un soggetto voglia rivelare a determinati individui, ma non ad altri.[16][17]

1.2 Aspettativa di privacy nello spazio pubblico

"The reasonable expectation of privacy" è un concetto giuridico che nasce negli Stati Uniti nel Ventesimo secolo, ad opera della giurisprudenza. Fondamentale per la tutela della privacy nell'ordinamento statunitense è il Quarto Emendamento, il quale recita "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized". Tale emendamento protegge l'individuo da perquisizioni e sequestri non autorizzati.

Centrale in tale contesto è la sentenza *Katz v. United States*[18] del 1967: il caso di specie riguardava un cittadino che aveva subito delle intercettazioni, senza previa autorizzazione, in una cabina telefonica ad opera della polizia. Rigettando la posizione del governo che, ispirandosi al noto precedente *Olmstead v. United States*, sosteneva la tesi secondo cui si poteva trattare di perquisizione solo nel caso in cui questa fosse avvenuta all'interno dell'abitazione di un soggetto, la *Supreme Court* sancisce che "the Fourth Amendment protects people, not places". Dunque, l'appellante, trovandosi in una cabina vetrata e chiusa, ciò che voleva evitare, non era l'essere non visto dal

[15] Austin Lisa, «Privacy and the question of technology», *Law and Philosophy* 22, n. 2 (2003): 119–66, http://www.jstor.org/stable/3505151.

[16] Jeffrey M. Skopek, «Reasonable Expectations of Anonymity», *Virgiania Law Review* 101, n. 3 (2015): 691–762, https://www.virginialawreview.org/articles/reasonable-expectations-anonymity/.

[17] Daniel J. Solovet, «Conceptualizing Privacy», *California Law Review* 90, n. 4 (2002): 1087–1155, https://doi.org/10.2307/3481326.

[18] Katz v. United States, 389 U.S. 347 (1967).

resto delle persone, ma che qualcuno ascoltasse la sua conversazione. Tale sentenza, oltre a costituire un precedente fondamentale, ha dato vita al test sulla ragionevole aspettativa di privacy, ad opera del giudice Harlan, che si compone di due parti: affinché sussista, la corte dovrà chiedersi in primo luogo se la persona ha effettivamente mostrato un'aspettativa di privacy e in secondo luogo se questa è riconosciuta dalla società come ragionevole. Se sono soddisfatti entrambi i requisiti, si potrà applicare la protezione offerta dal Quarto Emendamento anche in luoghi pubblici.[19]

Inoltre, anche a seguito della diffusione dell'utilizzo di database per l'archiviazione di dati personali, si è diffusa l'idea che la privacy proteggesse l'area personale di ciascuno dalle intrusioni che, governi e istituzioni pubbliche, potevano perpetrare. Tale percezione della privacy è dipesa dalla sua associazione all'area del diritto privato, sulla base della dicotomia tra le nozioni di "privato" e "pubblico". Ciò ha condotto molti studiosi a negare una privacy anche quando ciascuno si trova in aree pubbliche, tanto da considerare una tale concezione come paradossale.[20] Secondo Jeffrey Reiman la privacy "it does not assert the right never to be seen even on a crowded street": non si può parlare di protezione della privacy in pubblico, dal momento che quando si decide di esporsi al pubblico, sarebbe irragionevole pensare che si possa rendere non noto, un dato, nel momento cui si esce alla vista di tutti è già esposto volontariamente. Inoltre, nel momento in cui un soggetto decide di esporre pubblicamente un'informazione personale non può aspettarsi che venga vietato percepire o parlare in spazi pubblici, perché ciò costituirebbe una limitazione alla libertà altrui. Questo è quanto è stato ribadito anche nella sentenza *California v. Greenwood*[21] del 1988 dalla Corte Suprema, stabilendo nel caso di specie, che l'aver lasciato la spazzatura nel raccoglitore dei rifiuti implicasse averla lasciata in un luogo adatto all'ispezione pubblica e per questo gli appellanti non avevano alcuna aspettativa di privacy, in quanto avevano gettato via l'immondizia. [22][23] La privacy è un

[19] «If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine», *Harvard Law Review* 130, n. 7 (2017): 1924–45.

[20] Helen Nissenbaum, «Protecting Privacy in an Information Age: The Problem of Privacy in Public», *Law and Philosophy* 17, n. 5–6 (1998): 559–96, https://doi.org/10.2307/3505189.

[21] California v. Greenwood, 486 U.S. 35 (Supreme Court of United States 1988).

[22] H. Jeffrey Remain, «Privacy, Intimacy, and Personhood», *Philosophy & Public Affairs* 6, n. 1 (1976): 44, https://www.jstor.org/stable/2265060.

interesse fondamentale, ma deve essere bilanciato con altri interessi: ciò la pone in secondo piano in determinate occasioni.

La *Supreme Court* ha elaborato due dottrine che escludono l'applicazione del Quarto Emendamento: si tratta della "*third party doctrine*" e della dottrina della "*plain view*". Secondo la prima non ci può essere una ragionevole aspettativa di privacy nel momento in cui determinate informazioni sono rese note a terzi, anche se in modo confidenziale. Questo è quanto è emerso nella sentenza *United States v. Miller*[24] del 1976, dove è stato stabilito che il Quarto Emendamento non si applica alle registrazioni bancarie. La dottrina della "*plain view*", invece, prevede che non sia applicata la tutela da perquisizioni e arresti, nel caso in cui, ciò che la polizia osserva, è ciò che qualsiasi persona potrebbe osservare. La sua applicazione la si ritrova in un'altra famosa sentenza, *Florida v. Riley*[25] del 1989, dove la Corte Suprema ha stabilito che non si trattasse di una violazione di privacy l'aver osservato dall'alto con un elicottero la presenza di piante di marijuana all'interno di una proprietà privata, dal momento che sarebbe irragionevole pensare che la polizia non possa guardare all'interno, così come fanno generalmente le persone che prendono abitualmente aerei.[26]

Le persone non si aspettano di avere lo stesso grado di privacy in pubblico e in privato, ma stabilire cosa si intenda per luogo pubblico appare controverso: nella tradizione statunitense pubblico è qualsiasi luogo che sia alla vista di chiunque, dunque anche un giardino di una casa, nel caso esso sia visibile da fuori. Prevedere che la privacy sussista solamente nei luoghi privati risulta essere pericoloso. Ad influire nell'individuazione di luogo pubblico incidono determinati fattori, quali la dispersione delle informazioni, l'anonimato, che garantisce ad un soggetto di non essere individuato, l'avvento delle tecnologie. Tutelare la privacy in pubblico risulta essere fondamentale anche per il rispetto della dignità e del principio di uguaglianza: Alan Westin sostiene che garantire la privacy solo all'interno di luoghi privati aumenta le discriminazioni tra soggetti che vivono in quartieri poveri e sovraffollati e

[23] «California v. Greenwood, 486 U.S. 35 (1988)», Justia Law, consultato 25 ottobre 2021, https://supreme.justia.com/cases/federal/us/486/35/.

[24] United States v. Miller 425 U.S. 435 (1976).

[25] Florida v. Riley, 488 U.S. 445 (1989).

[26] Skopek, «Reasonable Expectations of Anonymity».

persone benestanti, dal momento che i primi individuano la necessità di uscire in luoghi pubblici per ritagliarsi la loro intimità, devono utilizzare mezzi pubblici per muoversi, esponendosi così maggiormente alla sorveglianza di massa.[27]

1.3 Necessità di un nuovo ripensamento dello spazio pubblico alla luce dello sviluppo dell'AI

L'avvento delle nuove tecnologie ha comportato la diffusione di un bisogno ancora più intenso di protezione della privacy da parte degli individui.

Gli studi scientifici hanno condotto alla realizzazione di un grande progresso nello sviluppo di questi nuovi apparati tecnologici, che seppur molto utili nella vita di tutti i giorni, sono percepiti anche come minaccia alla propria privacy.

Quel che si può avvertire costantemente è che le informazioni che un tempo erano riservate, attualmente, grazie a tali mezzi, risultano accessibili dalla pluralità dei soggetti.

In una sentenza del 2001, *Kyllo v. United States*, la *Supreme Court*, e in particolare il *giudice Scalia*, si sono espressi sostenendo come, l'uso di un dispositivo di *imaging* termico per individuare degli oggetti, non consiste in qualcosa di uso comune, e pertanto il suo utilizzo, privo di mandato, non rispetta il Quarto Emendamento.[28] In quest'ottica il concetto di "reasonable expectation of privacy" è influenzato dal modo in cui le nuove tecnologie vengono impiegate: rientra in tale nozione, dunque, solo ciò che le persone dovrebbero ragionevolmente aspettarsi come privato.

Un ulteriore caso in cui la Corte Suprema si è espressa negativamente sull'utilizzo di tali nuovi mezzi, è il caso *United States v. Jones* del 2012, in cui un soggetto, sospettato di essere trafficante di droga, ha ricorso contro la polizia per aver posto un localizzatore GPS nella sua auto al fine di individuarne gli spostamenti. Secondo l'opinione della maggioranza anche in questo caso la polizia ha violato il Quarto Emendamento.[29]

---

[27] Elizabeth Paton-Simpson, «Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places», *The University of Toronto Law Journal* 50, n. 3 (2000): 305–46, https://doi.org/10.2307/825907.

[28] Kyllo v. United States, 533 U.S. 27 (2001).

[29] United States v. Jones, 565 U.S. 400 (2012).

Attualmente i software di sorveglianza pubblica che risultano essere più diffusi sono software di riconoscimento facciale. Sono presenti in molte tecnologie che le persone usano quotidianamente; basti pensare alle modalità di sblocco delle schermate di pc e smartphone. Tutti questi mezzi catturano informazioni che risultano molto rilevanti per la tutela della privacy, quindi, risulta di primaria importanza regolare la loro accessibilità.[30]

La nascita della tecnologia ha dunque permesso che l'anonimato di cui il soggetto gode quando è in pubblico, esistente anche se può essere notato tra la folla, venga eroso dal fatto che i nuovi mezzi hanno la capacità di acquisire e collezionare molti dati, che possono essere confrontati con i dati presenti nei propri database, mediante l'uso di algoritmi. È noto l'esperimento condotto nel 2013 da un professore dell'Università di Carnegie Mellon, Alessandro Acquisti, il quale, una volta fotografati studenti nel campus, utilizzando un programma gratuito, è riuscito a ottenere delle informazioni personali, compresi i numeri di previdenza sociale.[31]

La ragionevole aspettativa di privacy risulta essere ridotta dalla semplicità con cui ciascuno può accedere a numerosi dati personali di altri individui. I tribunali in alcune sentenze hanno delineato come sia necessario articolare livelli diversi di trasparenza nell'accessibilità di informazioni raccolte pubblicamente: si può notare che in alcuni casi è stata vietata la divulgazione di dati personali, come nel caso di accesso ai fascicoli degli arrestati da parte di giornalisti, mentre in altri hanno ammesso l'accesso, ovvero per la divulgazione dei nomi dei soggetti che avevano firmato una petizione.[32]

La trasparenza delle informazioni personali può avere però due impatti: uno negativo, di minaccia della democrazia costituzionale, sia dal punto di vista istituzionale che dell'individuo, in quanto viene meno la tutela della libera manifestazione di pensiero dei cittadini, della libera associazione, riunione e del discorso anonimo, così come protetti dal Primo Emendamento della costituzione degli USA, il quale sancisce "Congress shall make no law respecting an establishment of

[30] Joel R. Reidenberg, «Privacy in Public», *University of Miami Law Review* 69, n. 1 (2014), https://repository.law.miami.edu/umlr/vol69/iss1/6.

[31] «"Big Brother" is big business?», CBS News, 2013, https://www.cbsnews.com/news/big-brother-is-big-business/.

[32] Reidenberg, «Privacy in Public».

religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances": mediante l'uso di dispositivi di sorveglianza il governo penetra l'anonimato di coloro che si impegnano in condotte espressive in pubblico, andando ad influenzare il comportamento di chi ha il desiderio di rimanere anonimo; e uno positivo, conservare valori democratici, in quanto può far sì che i funzionari pubblici si sentano più responsabili nello svolgimento del proprio lavoro, in quanto le attività svolte risultano essere di dominio pubblico, grazie all'accessibilità a tutti i cittadini.

Per controllare le informazioni che possono essere rese accessibili e trasparenti al resto della società è necessario individuare cosa possa essere classificato di rilevanza pubblica e cosa no.[33][34]

Lo sviluppo di tali nuovi sistemi, combinati con la profilazione, che è resa possibile dai numerosi dati condivisi in siti internet, motori di ricerca e social networks, riduce l'aspettativa di privacy nello spazio pubblico. Pertanto, è necessario individuare un apparato di norme che vada a regolamentare l'uso di tali sistemi informatici, onde evitare che con il passare del tempo ciò possa condurre a violazioni di principi cardine del costituzionalismo e diritti fondamentali delle società democratiche, protetti dalle carte costituzionali, quali la libertà di manifestazione di pensiero e di opinione, la libertà di associazione e di riunione. A tutela di tali diritti si è posta la corte nel caso *Gibson v. Florida Legislative Investigation Committee*[35] del 1963, la quale ha riconosciuto la necessità di tutelare l'identità dei membri appartenenti ad un gruppo, al fine di tutelare il diritto costituzionale alla libera associazione. La divulgazione dei nomi avrebbe costituito una minaccia per la privacy.[36]

Prova di quanto potrebbe anche accadere anche nei regimi democratici, è accaduto nelle proteste di Hong Kong del 2019 quando i manifestanti hanno coperto il proprio volto con degli ombrelli, onde evitare che la polizia mediante sistemi di

[33] Christopher Slobogin, «Public Privacy: Camera Surveillance of Public Places And The Right to Anonymity», *SSRN Electronic Journal*, 24 febbraio 2003, https://doi.org/10.2139/ssrn.364600.

[34] Reidenberg, «Privacy in Public».

[35] Gibson v. Florida Legislative Investigation Committee, 372 U.S. 539 (United States Supreme Court 1963).

[36] Paton-Simpson, «Privacy and the Reasonable Paranoid».

riconoscimento facciale potesse individuarli.[37] Allo stesso modo in Russia il governo ha usato sistemi di riconoscimento facciale presenti in metal detector posti all'accesso della protesta autorizzata, per individuare manifestanti che si opponevano all'arresto di Alexei Navalny.[38] Inoltre Mosca ha deciso di adottare un sistema di riconoscimento facciale in tutta la città e nelle scuole.

I sistemi di sorveglianza, oltre ai numerosi risvolti legati alla violazione di privacy, sono impiegati anche per altri scopi. A seguito degli attentati terroristici, sono stati sfruttati da sistemi investigativi dei diversi paesi per individuare possibili minacce nelle città. O ancora, lo sviluppo dell'Artificial Intelligence (AI) ha permesso a molte società di sfruttare i numerosi dati che i soggetti producono mediante l'uso di pc, smartphone o altre tecnologie, per fini economici.

Ma ciò che effettivamente emerge è che queste tecnologie non sono ancora state oggetto di una regolamentazione che vada a disciplinare la loro utilizzazione nelle aree pubbliche.

In UE si sta discutendo di un regolamento sottoposto alla Commissione ad aprile 2021, da parte del Parlamento Europeo, volto a disciplinare l'uso dell'AI nei diversi settori pubblici. I sistemi biometrici sono considerati come sistemi ad alto rischio, per questo il loro utilizzo deve essere limitato.

Questa diffusione di strumenti di AI ha reso i soggetti più vulnerabili, ha fatto sì che l'anonimato di cui si godeva un tempo, che garantiva che un evento non venisse associato a un determinato individuo o gruppo, risultasse indebolito da tali mezzi, in quanto in grado di rendere probabile ciò che un tempo era improbabile: l'individuazione di molte informazioni personali e la relativa conservazione.

[37] Zak Doffman, «Hong Kong Exposes Both Sides Of China's Relentless Facial Recognition Machine», Forbes, 2019, https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/.

[38] Anastasia Zoblina, «Moscow's Use of Facial Recognition Technology Challenged», *Human Rights Watch* (blog), 2020, https://www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged.

2. LA DIFFUSIONE DI SISTEMI DI RICONOSCIMENTO FACCIALE

2.1 Cos'è il riconoscimento facciale

Le tecnologie di riconoscimento facciale (TRF) appartengono al settore dell'AI. L'AI è stata recentemente definita dall'*High-level group on artificial intelligence*, istituito dalla Commissione Europea nel 2019, come "software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal".[39] La nozione così delineata richiama quella di John McCarthy, che si ritiene aver coniato il termine: egli riteneva che l'Artificial Intelligence per essere descritta deve essere connessa all'intelligenza umana, della quale la prima si rende sua emulatrice.[40]

Il funzionamento dell'AI si basa su algoritmi: sequenze di istruzioni, rivolte ai sistemi di AI, che indicano quali operazioni compiere per raggiungere un determinato scopo.

Le TRF sono sistemi biometrici che sfruttano dunque un algoritmo, al fine di identificare un soggetto sulla base del suo volto, ripreso da un video o da fotografie, che viene confrontato con immagini della stessa persona che sono già presenti in un database. Alcuni Big Tech, come Amazon, Microsoft e IBM, hanno elaborato algoritmi di riconoscimento facciale, basati sugli studi del linguaggio non verbale degli anni 60' dello psicologo Paul Ekman, che delineò sei emozioni universali, uguali ovunque nel mondo a prescindere dal contesto sociale: rabbia, disgusto, paura, felicità e tristezza. Ciò che non era chiaro all'epoca, è che invece questi stati, espressioni

---

[39] «A Definition of Artificial Intelligence: Main Capabilities and Scientific Disciplines» (Brussels: European Commission, 2019), https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines.--

[40] John McCarthy, «What is Artificial Intelligence? », 12 Novembre 2007, http://jmc.stanford.edu/articles/whatisai.html.

cambiano a seconda del contesto culturale in cui si nasce e cresce e dalla circostanza in cui un individuo si può trovare.[41]

Rispetto agli altri sistemi biometrici, quali per esempio le impronte digitali o il DNA, le TRF risultano di più facile utilizzo. Si tratta di sistemi che sono costituiti da dispositivi in grado di compiere prestazioni in modo sempre più efficiente e preciso, il cui costo, con l'ampia diffusione a cui si assiste, risulta essere sempre più accessibile a chiunque. Le telecamere sono in grado di rilevare immagini da centinaia di metri, alla luce del giorno ma anche di notte, e di individuare se i movimenti registrati sono fuori dall'ordinario così da dare un allarme. Sono inoltre inseriti in molti dispositivi che usiamo quotidianamente: pc, smartphone e smart TV.[42][43]

Le TRF, come anche i sistemi di AI, utilizzano i *big data*, la cui definizione non indica semplicemente un gran numero di dati, ma è riconducibile alle c.d. tre V: "volume" di dati raccolti, "varietà" delle fonti da cui provengono i dati e "velocità" di produzione analisi e di dati. Questi hanno generato negli ultimi due decenni una digital economy: basti pensare che Facebook acquisisce ogni giorno circa 350 milioni di nuove foto, caricate dai suoi due miliardi di utenti. In questo modo affina sempre più i suoi sistemi di AI, che sono sempre più in grado di riconoscere cosa sia presente in ciascuna foto, ricavando informazioni preziose per le aziende e veicolando così gli annunci per ciascun soggetto.[44] Questo sistema di Face Recognition usato da Facebook, a causa delle crescenti preoccupazioni sull'uso di tale strumento, ha subito un arresto il 3 Novembre 2021. Secondo quanto riportato da Meta, la holding che fa capo a Mark Zuckemberg, i profili di riconoscimento, che permettono all'utente che utilizza il social network di ricevere suggerimenti sull'identità delle persone presenti

[41] Lisa Feldman Barrett et al., «Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements», *Psychological Science in the Public Interest* 20, n. 1 (2019), https://journals.sagepub.com/doi/10.1177/1529100619832930.

[42] Giuseppe Mobilio, *Tecnologie di riconoscimento facciale* (Napoli: Editoriale Scientifica s.r.l., 2021).

[43] Slobogin, «Public Privacy: Camera Surveillance of Public Places And The Right to Anonymity».

[44] Jared Bennet, «Saving face: Facebook wants access without limits», Center for Public Integrity, 2017, https://publicintegrity.org/inequality-poverty-opportunity/saving-face-facebook-wants-access-without-limits/.

nelle foto che posta, saranno cancellati, almeno fintantoché le autorità non avranno stabilito regolare chiare.[45]

La disponibilità di *big data* sta aumentando sempre più a causa della continua creazione di app e nuovi social networks e alla costante condivisione di informazioni personali. In un report del *U.S. Government Accountability Office* del 2020, è riportato che nei prossimi anni il mercato delle TRF sarà destinato ad aumentare: dal 2016 al 2019 i dati acquisiti con le TRF hanno prodotto tra 3-5 miliardi di dollari, mentre si pensa che dal 2022 al 2024 potrebbe aumentare di 7-10 miliardi di dollari. Secondo alcuni studiosi i dati sono diventati la "nuova valuta" dell'economia digitale.[46]

La *computer vision* si occupa dell'analisi di immagini mediante l'utilizzo di un calcolatore, per individuare cosa sia presente in una scena e dove. A seguito degli sviluppi tecnologici si è passati da un sistema *top-down*, dove era l'uomo ad indicare all'algoritmo cosa ricavare dalla foto, ad un sistema *botton-up*, dove gli algoritmi sono "allenati" per imparare in autonomia ed estrarre le caratteristiche dei volti dei soggetti più ricorrenti, sulla base di enormi quantità di dati già catturati: si parla in questo secondo caso di *machine learning*. I sistemi di TRF si basano sull'individuazione di *patterns*, usati all'interno di dati per il *training* degli algoritmi e sul confronto tra nuovi dati con schemi precedenti, al fine di individuare ricorrenze e predire nuove correlazioni. [47]

Il *machine learning* ha avuto successo anche grazie alla nascita delle *Artificial Neural Network* (ANN): sistemi di elaborazione dei dati basati su una struttura fisica e su una logica di funzionamento diverse dai computer classici, che riproduce il modello del sistema nervoso del cervello e delle reti neurali appunto. Queste hanno condotto alla costituzione del *deep learning*, una sottocategoria del machine learning: si tratta

[45] Elizabeth Dwoskin e Drew Harwell, «Facebook Is Ending Use of Facial Recognition Software, Deleting Data on More than a Billion People», *Washington Post*, 3 novembre 2021, https://www.washingtonpost.com/technology/2021/11/02/facebook-ends-facial-recognition/.

[46] «Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses» (United States Government Accountability Office, 2020), https://www.gao.gov/products/gao-20-522.

[47] Mobilio, *Tecnologie di riconoscimento facciale*.

di un sistema in cui il risultato è frutto di una comunicazione tra i diversi livelli nella rete.[48]

Alla luce dei progressi di queste nuove tecnologie si assiste ad una sempre più crescente difficoltà da parte dell'uomo di individuare il percorso seguito dalla macchina.

Le TRF nell'"analisi facciale" seguono un procedimento che si divide in più fasi:

a. *Acquisizione dell'immagine*: il volto di una persona viene catturato in video o foto e trasformato in formato digitale.
b. *Individuazione del volto*: l'immagine della persona viene distinta dallo sfondo.
c. *Normalizzazione*: operazione volta ad uniformare le immagini, migliorandone la qualità.
d. *Estrazione delle caratteristiche*: processo volto a isolare ed estrarre le caratteristiche biometriche distintive del volto di una persona.
e. *Registrazione*: conservazione dell'immagine o del modello biometrico in un database.
f. *Confronto*: operazione che paragona le caratteristiche o i tratti biometrici di un modello di riferimento con altri già registrati.

Le TRF possono essere usate per finalità diverse:

- *Verificazione/Autenticazione*: si tratta della comparazione uno-a-uno, che può applicarsi confrontando l'immagine catturata con quelle di una persona già nota, tipico caso che si realizza negli aeroporti, dove si controlla il passaporto (verifica); oppure se non si conosce l'identità del soggetto, si verifica se la stessa persona nell'immagine sia presente anche in un'altra immagine.
- *Identificazione*: si tratta di una comparazione uno-a-molti, dove l'immagine del volto di una persona sconosciuta viene confrontata con quelle di altre persone note presenti in una galleria.
- *Categorizzazione*: estrazione delle caratteristiche di un soggetto, al fine di classificarla in una o più categorie sulla base di queste. L'obbiettivo non è dunque l'individuazione del singolo.

[48] Giovanni Ziccardi e Pierluigi Perri, *Tecnologia e diritto. Informatica e diritto. Data governance, protezione dei dati e gdpr, mercato unico digitale, blockchain, pubblica amministrazione digitale*, vol. 2 (Giuffrè Francis Lefebvre, 2019).

Nonostante i diversi sviluppi delle TRF, divenuti sempre più precisi, persiste comunque la possibilità di una percentuale variabile di errore, dipeso da calcoli probabilistici effettuati dall'algoritmo per individuare il soggetto, il quale ad ogni ricerca può elaborare una pluralità di dati. Ad incidere nella precisione dei risultati ottenuti emergono: la qualità e la risoluzione dell'immagine, il riflesso della luce, il movimento della persona, la posa del volto, ma anche l'età, il tipo di pelle, la presenza di trucco o l'acconciatura dei capelli. Nel migliore dei casi il tasso d'errore può arrivare ad un livello inferiore al 0.1%; al contrario nel caso in cui l'identificazione avvenga in ambienti non controllati questa può arrivare ad un tasso di errore del 2.8%.[49]

I modelli di sorveglianza mediante l'uso delle TRF adottati dai governi, vanno oltre il modello elaborato da Jeremy Bentham nel *Panopticon*: non si tratta più di un unico "ispettore" posto su una torre in grado di sorvegliare i detenuti, ma di un intero sistema di videocamere, poste ovunque nelle città, in grado di visionare ogni cosa e di raccogliere un'enorme quantità di dati.

2.2 Diritti fondamentali colpiti dall'uso di TRF

L'utilizzo delle TRF può incidere sulle libertà delle persone, rischiando di ledere alcuni dei diritti fondamentali. Questo può accadere, in modo più evidente, se vengono impiegate in spazi pubblici: si genera quello che è noto come *chilling effect*, ovvero il soggetto è scoraggiato nell'esercizio delle proprie libertà, per il timore di essere ripreso e subire sanzioni. Nel 2013 uno studio realizzato sulle comunità musulmane di New York e New Jersey ha evidenziato come l'eccessiva sorveglianza della polizia su appartenenti alla comunità ha avuto un effetto frenante: le persone si sentivano meno libere di esercitare quelle libertà garantite dal Primo Emendamento, quali la libertà di espressione, di religione, di associazione, riunione.[50]

[49] Mobilio, *Tecnologie di riconoscimento facciale*; Patrick Grother, Mei Ngan, e Kayee Hanaoka, «Face Recognition Vendor Test (FRVT) Part 2: Identification», NIST Interagency/Internal Report (NISTIR) (National Institute of Standards and Technology, Gaithersburg, 2019), https://doi.org/10.6028/NIST.IR.8271; Javier Galbally Herrero et al., «Study on Face Identification Technology for Its Implementation in the Schengen Information System» (Lussemburgo: Publications Office of the European Union, 2019), https://publications.jrc.ec.europa.eu/repository/handle/JRC116530.

[50] Diala Shamas e Nermeen Arastu, «Mapping Muslims: NYPD Spying and its Impact on American Muslims», marzo 2013, http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.; Commitee

La reazione delle persone a tale uso è diversa tra il continente europeo e quello statunitense: in USA, sebbene si assista ad una diffidenza nell'uso di tali mezzi in alcune comunità, la maggior parte delle persone ha fiducia nell'uso di queste tecnologie negli spazi pubblici, mentre in UE solo il 17% è favorevole all'uso di sistemi di TRF da parte delle pubbliche amministrazioni per la registrazione del proprio volto in database.

Uno studio effettuato dai ricercatori di Georgetown del 2016 ha evidenziato come negli USA un americano su due è già presente in un database accessibile alle forze dell'ordine.[51]

L'uso di TRF dal vivo, senza un previo consenso informato, pone le persone in una posizione debole e potenzialmente umiliante. Ma ad essere lesa è soprattutto la dignità umana, fondatrice degli altri diritti garantiti dalla Dichiarazione universale dei diritti dell'uomo del 1948.

Se le persone sono a conoscenza del fatto di essere sottoposte a TRF, possono sentirsi non libere nei luoghi pubblici e ancor di più se queste vengono impiegate in gradi eventi pubblici, dal momento che ciò può comportare l'individuazione di molte persone. È necessario che la polizia tenga un comportamento adeguato, al fine di non porre la persona in una situazione di disagio: risulterebbe fondamentale dunque predisporre una formazione anche per le autorità che si accingono a sfruttarne le potenzialità, onde evitare che si possano realizzare abusi.[52]

La Carta dei diritti fondamentali dell'Unione Europea disciplina all'art. 52 i casi, strettamente necessari, in cui può realizzarsi una limitazione dei diritti fondamentali. La disposizione prevede che questa può avvenire solo se:

- È previsto dalla legge.
- Risponde ad obbiettivi di interesse generale.
- Protegge altri diritti fondamentali, senza ignorarli.
- Rispetta l'essenza del diritto.

of Ministers, «Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies» (Council of Europe, 11 giugno 2013), https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c8011.

[51] Clare Garvie, Alvaro Bedoya, e Jonathan Frankle, «The Perpetual Line-Up», *Privacy & Technology at Georgetown Law*, 18 ottobre 2016, https://www.perpetuallineup.org/.

[52] «Facial recognition technology: fundamental rights considerations in the context of law enforcement» (FRA European Union Agency for fundamental Rights, 27 novembre 2019).

- È proporzionata.

La Corte di Giustizia si è espressa in merito al principio di proporzionalità stabilendo come la sua applicazione debba essere valutata caso per caso e come si inserisca in un iter valutativo ampio che va a verificare se l'obbiettivo legittimo stabilito dalla norma viene rispettato. La stessa posizione è abbracciata dalla Corte EDU, che nella sentenza *Marper*[53] ha sancito come una misura per essere applica debba essere necessaria all'interno di una società democratica per perseguire i fini indicati nell'art. 8 CEDU. Deve inoltre essere proporzionata allo scopo perseguito e le ragioni devono essere sufficienti e rilevanti. Ma nonostante ciò, l'atteggiamento della corte europea dei diritti dell'uomo appare alquanto oscillante: da un totale disappunto in merito all'utilizzo di tecnologie che appaiono troppo invasive nella sfera privata, non garantite da una base legale, come è emerso nella sentenza *Sommer v. Germany*[54] del 2017; si assiste ad una regressione delle tutele offerte a coloro i quali subiscono un'ingerenza delle autorità pubbliche, fino a ritenere compatibili con le garanzie della CEDU le intromissioni nella sfera individuale delle persone mediante sistemi informatici per l'interesse alla sicurezza nazionale, anche se prive di qualsiasi autorizzazione giudiziale.[55][56]

Quindi nel caso in cui uno stato voglia adottare nuove tecnologie, deve adottarle sulla base di un adeguato bilanciamento con gli altri interessi, che valuti la proporzionalità in relazione allo scopo perseguito. Tale considerazioni si rivengono anche nella Convenzione 108+ del Consiglio d'Europa. Essa, nota anche come Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, è stata stipulata nel 1981 a Strasburgo: ha visto la nascita di un regime per la protezione dei dati personali negli stati firmatari e una base per la disciplina europea. Si tratta di uno strumento giuridico, strutturato per principi e suscettibile di essere implementato, vincolante per gli stati che vi hanno aderito e aperto all'adesione di altre parti. Nel 2018 la Convenzione 108 è stata oggetto di

[53] S. & Marper v. UK (Corte Europea dei Diritti dell'Uomo 4 dicembre 2008).

[54] Sommer v. Germany (Corte europea dei diritti dell'uomo 27 aprile 2017).

[55] Federica Centorame, «Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona», *Rivista italiana di diritto e procedura penale*, n. 2 (2021): 517–23.

[56] Big Brother Watch e altri v. UK; (Corte europea dei diritti dell'uomo 13 settembre 2018).

innovazioni, in parallelo con la nuova disciplina dell'Ue: in virtù di ciò si parla di Convenzione 108+.[57]

2.2.1 Diritto al rispetto della vita privata e diritto alla protezione dei dati personali

Il diritto al rispetto della vita privata o diritto alla privacy, e il diritto alla protezione dei dati personali, sono diritti autonomi, ma che proteggono simili valori, come l'autonomia e la dignità umana. Il loro rispetto risulta fondamentale per garantire la sfera personale di ciascuno.

Il diritto al rispetto alla vita non presenta confini precisi e una definizione esaustiva. È garantito a livello internazionale nella Dichiarazione universale dei diritti umani del 1948, all'art. 12; nel continente europeo dalla CEDU all'art. 8, il quale sancisce il rispetto della vita privata e familiare e dalla Carta di Nizza all'art. 7. I due articoli presentano un contenuto similare; mentre nell'ordinamento statunitense non si rinviene una specifica normativa che tuteli la privacy: il Quarto Emendamento della costituzione americana può dirsi a tutela di questa.

Il rispetto della vita privata non implica la sola una protezione all'interno della propria abitazione, ma può trovare una tutela anche nello spazio pubblico: si tratta della ragionevole aspettativa di privacy, nozione elaborata dalla giurisprudenza statunitense e recepita anche dalla Corte EDU, secondo cui è garantito all'individuo uno spazio inaccessibile a sistemi di sorveglianza anche quando si trova in pubblico.[58]

Con l'avvento dell'era digitale e la conseguente ampia diffusione di internet, social network e app, si è reso necessario l'individuazione e l'istituzione di un nuovo diritto: il diritto alla protezione dei dati personali. Tuttavia, il concetto di dato personale non nasce con lo sviluppo della tecnologia: ciò su cui quest'ultima ha influito è la possibilità di una maggiore circolazione di informazioni personali. Infatti, i numerosi mezzi informatici acquisiscono dati degli utenti e compiono azioni di sorveglianza e controllo: tra questi le TRF sono tra le più invasive. La società sta infatti vivendo un'era che può essere indicata come "*dataveillance*" (*data-*

[57] S. & Marper v. UK (Corte Europea dei Diritti dell'Uomo 4 dicembre 2008); Jennifer Lynch, «Face Off: Law enforcement use of face recognition technology», febbraio 2018, https://www.eff.org/wp/face-off; Mobilio, *Tecnologie di riconoscimento facciale p.123-124*.

[58] «Katz v. United States, 389 U.S. 347 (1967)».

surveillance): i dati personali vengono impiegati in modo sistematico per indagare o monitorare le azioni o le comunicazioni delle persone.[59] Ciò non implica automaticamente che ciò abbia un'accezione negativa di sorveglianza, perché può portare vantaggi per il mantenimento della sicurezza pubblica, per un controllo dell'azione dei governanti da parte dei cittadini e per l'economia. Potendo monitorare costantemente il comportamento umano e le dinamiche sociali, prevedendole, si viene a creare una nuova entità, un'entità digitale, tanto da poter ipotizzare la creazione di una nuova categoria giuridica, l'*habeas data*, proprio al fine di proteggerne i diritti in tale realtà.[60]

La conservazione e l'uso di dati personali e immagini delle persone richiedono la sottoposizione ad un test, che verifichi la sussistenza di requisiti, quali la necessità e la proporzionalità, e che tenga conto del fine perseguito, del contesto e delle circostanze.

È in ambito europeo che tale diritto viene per la prima volta istituzionalizzato: il diritto alla protezione dei dati personali si distingue dal diritto alla privacy, anche se detiene un ruolo fondamentale nella garanzia di questa. Si rinviene una distinta disciplina dei due diritti in due articoli differenti: l'art. 7 della Carta dei diritti fondamentali sancisce la protezione della vita privata e familiare, mentre l'art. 8 disciplina la protezione dei dati personali. Una più mirata e completa tutela del trattamento dei dati personali si può rinvenire solo con il regolamento dell'Unione Europea n. 2016/679, il *General Data Protection Regulation* (GDPR), in vigore dal 25 maggio 2018, il quale disciplina la libera circolazione delle informazioni digitali e la loro tutela. L'art.9 sancisce che il trattamento di dati biometrici è consentito solo se "necessario per motivi di interesse pubblico rilevante, sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure adeguate e specifiche per la salvaguardia dei diritti fondamentali e degli interessi della persona interessata". Il GDPR prevede che l'acquisizione e l'elaborazione di immagini debba rispettare determinati requisiti: essere legale, equa e trasparente, seguire uno scopo specifico, esplicito e legittimo e rispettare i parametri di

[59] Roger Clarke, «Information technology and dataveillance», *Communications of the ACM* 31, n. 5 (1 maggio 1988): 498–512, https://doi.org/10.1145/42411.42413.

[60] Mobilio, *Tecnologie di riconoscimento facciale, p. 79*.

minimizzazione di dati, accuratezza dei dati, limitazioni della conservazione, sicurezza dei dati e responsabilità.

La disciplina del trattamento dei dati personali però non ha trovato lo stesso riconoscimento, quale diritto inviolabile dell'uomo, nel resto del mondo. In alcuni paesi si assiste al tentativo di generare una disciplina, che per lo meno si avvicini al modello europeo. Primo tra tutti è lo stato della California, il quale, a seguito dell'entrata in vigore nel 2018 del GDPR, ha emanato il *California Consumer Privacy Act* (CCPA) in vigore dal 2020. Sempre negli USA, una simile disciplina della materia è stata introdotta dalla Virginia con il *Consumer Data Protection Act* (CDPA), che entrerà in vigore da gennaio 2023.[61] Ma negli Stati Uniti manca una legislazione a livello federale che vada a tutelare tale diritto: si tratta di uno scenario normativo frammentato. Altri paesi hanno approvato una legge sulla protezione dei dati personali, il Brasile per esempio ha emanato *la Lei Geral de Proteção de Dados Pessoais* (LGPD).

2.2.2 Diritto di non discriminazione

L'utilizzo delle TRF può comportare anche la violazione del principio di uguaglianza: sia dal punto di vista formale che dal punto di vista sostanziale.

Il divieto di discriminazioni si può rinvenire in plurime carte costituzionali e convenzioni internazionali: in UE l'art. 21 della Carta dei diritti fondamentali dei cittadini sancisce al co. 1 "È vietata qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, la disabilità, l'età o l'orientamento sessuale.", mentre al co.2 "Nell'ambito d'applicazione dei trattati e fatte salve disposizioni specifiche in essi contenute, è vietata qualsiasi discriminazione in base alla nazionalità." Simile contenuto lo si rinviene nella CEDU agli artt. 12 e 14, anche se con una portata meno ampia.

[61] McGuireWoods LLP-Janet P. Peyton, «Virginia's New Consumer Data Protection Act (CDPA)», Lexology, 4 marzo 2021, https://www.lexology.com/library/detail.aspx?g=adaf6e67-d384-4aa5-a50b-ad8e31f43d8c.

Negli Stati Uniti invece una protezione del principio di uguaglianza lo si può rinvenire nel Quattordicesimo Emendamento, dove è sancita una pari protezione di tutti i soggetti.

Nonostante tale riconoscimento generalizzato nei due ordinamenti, è principio generalmente ammesso anche il fatto che può sussistere un trattamento diverso e meno favorevole, nel caso in cui ciò sia supportato da valide motivazioni.

Si parla di violazione del principio di uguaglianza dal punto di vista formale nell'uso delle TRF, nel caso in cui la discriminazione dipenda da un errore compiuto dall'algoritmo, che può ricondursi alla fase di *design* o anche alla fase decisionale. Queste distorsioni, o *bias*, generano falsi-positivi o falsi-negativi.[62] Emblematici in tal senso sono, sotto il profilo razziale, i casi statunitensi di arresti di persone afroamericane compiuti sulla base di errori dell'algoritmo e dovuti ad un *training* per il riconoscimento di volti principalmente realizzato con immagini di persone bianche. Ciò conduce quindi ad una minor precisione nel caso in cui venga applicato a persone nere.[63] È noto in merito lo studio compiuto dalla ricercatrice Joy Buolamwini del gruppo Civic Media del MIT Media Lab che ha portato alla luce come si verificassero delle discriminazioni operate dall'algoritmo nel momento in cui queste andavano a scansionare volti di persone nere piuttosto che bianche.[64]

Dal punto di vista sostanziale invece, ciò che emerge è la necessità che le autorità pubbliche si impegnino affinché a ciascun soggetto possano essere garantiti gli stessi diritti. L'uso delle TRF può comportare una lesione di diritti fondamentali dei soggetti che principalmente si trovano in una posizione di debolezza. È il caso, per esempio, del lavoratore che si trova ad essere analizzato durante un colloquio di lavoro: espressioni facciali come alzare le sopracciglia, stringere le labbra, alzare il mento, o il contatto visivo, il tono della voce sono tutti elementi usati dalle aziende che usano sistemi di riconoscimento facciale per valutare i candidati, non basandosi semplicemente sulla lettura del Curriculum Vitae, ma ottenendo indicatori affidabili privi di pregiudizi umani. Però se da un lato ciò porta numerosi vantaggi, quali

[62] Mobilio, *Tecnologie di riconoscimento facciale*.

[63] Kashmir Hill, «Wrongfully Accused by an Algorithm», *The New York Times*, 24 giugno 2020, par. Technology, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[64] Larry Hardesty, «Study finds gender and skin-type bias in commercial artificial-intelligence systems», MIT Media Lab, 11 febbraio 2018, https://www.media.mit.edu/articles/study-finds-gender-and-skin-type-bias-in-commercial-artificial-intelligence-systems/.

velocità, possibilità di intervistare un numero maggiore di candidati, assenza di preconcetti, ciò favorirà solo coloro che si rivelano abili nell'affrontare i colloqui in video, con il rischio di escludere quelle persone che in realtà sarebbero state più competenti nel lavoro.[65] Ma non solo, la lesione del principio di uguaglianza si realizza anche nel caso in cui le TRF siano installate nelle città, nei luoghi pubblici, e a venir tutelati in misura minore saranno i soggetti più poveri, i quali non dispongono di ampi spazi dove vivere la propria intimità, cosicché la cercheranno all'esterno della propria abitazione, risultando più vulnerabili rispetto alle persone che dispongono di più mezzi economici, in quanto il loro volto sarà sempre più facilmente accessibile a tali sistemi e alle autorità pubbliche.[66]

2.2.3 Diritti del bambino e dell'anziano

I sistemi di riconoscimento facciale possono risultare più pericolosi e più dannosi per determinate categorie di soggetti, che i legislatori considerano a priori più vulnerabili: si tratta di minori, anziani e disabili.

Per quanto attiene al minore, a livello normativo, si può rinvenire l'art. 24 della Carta dei diritti fondamentali dell'UE, che disciplina i diritti dei minori, prevedendo che questi debbano essere considerati un interesse primario e superiore. Inoltre, ampia tutela la si ritrova nella Convenzione delle Nazioni Unite sui diritti dell'infanzia del 1989, la quale prevede, tra i diritti fondamentali del minore, la superiorità dell'interesse del bambino.

Ciò che caratterizza la situazione del minore è la sua mancanza di consapevolezza nell'uso di tali strumenti e nella sottoposizione a essi.[67] Ogni giorno usano social networks condividendo immagini e informazioni personali che vengono salvate in database; contemporaneamente sono soggetti all'uso di TRF negli spazi pubblici. Nelle scuole, per esempio, la giustificazione di tali utilizzi può essere la più varia: per

[65] Charles Hymas, «AI used for first time in job interviews in UK to find best applicants», *The Telegraph*, 27 Settembre 2019, https://www.telegraph.co.uk/news/2019/09/27/ai-facial-recognition-used-first-time-job-interviews-uk-find/.

[66] Paton-Simpson, «Privacy and the Reasonable Paranoid».

[67] Lindsey Barrett, «Ban Facial Recognition Technologies for Children—And for Everyone Else», *Boston University Journal of Science and Technology Law* 26, n. 2 (24 luglio 2020), https://ssrn.com/abstract=3660118.

fini di sicurezza contro le sparatorie, per controllare la frequenza degli alunni o anche per valutare il grado di coinvolgimento nella didattica. Ma non solo, il 18 ottobre 2021 si è assistito in UK al lancio di una tecnologia di riconoscimento facciale da applicare nelle scuole al fine di velocizzare il pagamento del pranzo degli alunni. Una settimana dopo, il 25 ottobre, è stata resa nota la decisione di sospendere l'uso di TRF nelle nove scuole del North Ayrshire, che avevano adottato tali sistemi, a seguito di indagini aperte dall'*UK's Information Commisioner's Office* (ICO). L'obbiettivo è quello di far sì che le scuole adottino delle tecnologie meno invadenti.[68] Tutto ciò può comportare ripercussioni a livello pedagogico e dubbi in ambito giuridico, in merito al consenso consapevole. È pertanto necessario che l'utilizzo di immagini di minori, e più in generale dei loro dati biometrici, sia sottoposto a verifiche di rispetto di principi di proporzionalità e necessità rigorosi.[69]

La maggiore o minore età può condurre nell'utilizzo di TRF a *bias*: si registra un incremento del tasso di errore nella corrispondenza di immagine del volto, generando falsi-positivi, superiore a quella di soggetti adulti. Nello specifico, alcuni test dimostrano che l'uso di TRF su bambini con età inferiore a 13 anni, produce un numero superiore di falsi-positivi rispetto agli adulti.[70]

L'utilizzo di sistemi di riconoscimento facciale però non ha solo effetti negativi, perché se usato nel rispetto di parametri stabiliti, può essere fondamentale per salvare il diritto all'identità e la vita di molti minori alle frontiere.[71]

Una protezione a livello europeo la si ritrova per quanto riguarda gli anziani all'art. 25 della Carta dei diritti fondamentali, mentre per quanto riguarda le persone disabili la si può rinvenire all'art. 38 co. 3. Quest'ultima risulta fondamentale per il fatto che ogni disabilità può avere specificità e caratteristiche differenziate; inoltre, negli studi volti ad ottimizzare l'uso delle TRF manca una parte riservata ad essi, che

[68] «Schools pause facial recognition lunch plans», *BBC News*, 25 ottobre 2021, par. Technology, https://www.bbc.com/news/technology-59037346.

[69] Mobilio, *Tecnologie di riconoscimento facciale*; Gary T. Max e Valerie Steeves, «From the Beginning: Children as Subjects and Agents of Surveillance», *Surveilance and Society* 7, n. 3/4 (giugno 2010), https://doi.org/10.24908/ss.v7i3/4.4152.

[70] «Facial recognition technology: fundamental rights considerations in the context of law enforcement».

[71] European Union Agency for Fundamental Rights, «Under watchful eyes: biometrics, EU IT systems and fundamental rights» (Lussemburgo, 2018).

provi a porre rimedio al fatto che possono esserci soggetti con sindromi craniofacciali o con tratti somatici alterati.

2.2.4 Diritto all'identità e alla libertà personale

Le TRF hanno un grande impatto anche nei confronti di tutti quei diritti della personalità. Tra questi spicca il diritto all'identità personale: diritto di ampio riconoscimento internazionale, che ha l'obbiettivo di tutelare il pieno sviluppo della persona e l'interesse della comunità a conoscere la reale identità del soggetto. Si tratta di una "libertà da", intesa come libertà a ricevere una corretta rappresentazione della propria persona, a cui si aggiunge una "libertà di", intesa nel senso di manifestazione del potere di autodeterminazione. In questo modo l'identità corrisponde alla "proiezione del soggetto nella società".[72] Il diritto all'identità personale si arricchisce anche del diritto all'identità genetica e all'identità sessuale. Ma non solo, nell'era della diffusione di internet si è via via sviluppato un diritto all'identità digitale, inteso quale strumento volto a facilitare il riconoscimento dell'utente e a garantire l'accesso in sicurezza e più facilmente a beni o servizi.[73] In queste ipotesi sta sempre più diffondendosi l'utilizzo di TRF per la verifica o l'autenticazione. Una delle caratteristiche dell'impiego di TRF in tali sistemi consta nella decontestualizzazione rispetto all'identità della persona: le caratteristiche del volto del soggetto vengono trasformate in dati e l'individuo perde così la sua identità. Il rischio che si corre è che il soggetto, una volta sottoposto a tali sistemi, perda la sua reale identità personale.[74]

Ma anche la libertà personale può risultare lesa dal massivo impiego di tecnologie di riconoscimento facciale. Sul piano internazionale è protetta all'art. 3 della Dichiarazione universale dei diritti umani che sancisce la libertà della persona. La CEDU riconosce la tutela a tale diritto all'art. 5, mentre la stessa previsione la si rinviene anche all'art 6 della Carta dei diritti fondamentali dell'Unione Europea. La

[72] Mobilio, *Tecnologie di riconoscimento facciale p. 60-67*.

[73] Gruppo di lavoro Articolo 29, «Parere 3/2012 sugli sviluppi nelle tecnologie biometriche», 27 aprile 2012, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2375294.

[74] «L'identificazione del corpo umano: profili bioetici della biometria», Comitato Nazionale per la Bioetica, 2010, http://bioetica.governo.it/it/pareri/pareri-e-risposte/l-identificazione-del-corpo-umano-profili-bioetici-della-biometria/.

mancanza di prestazione del consenso da parte del soggetto sottoposto a TRF suscita dubbi in merito al rispetto della libertà personale: l'individuo che si trovi ad essere soggetto a sistemi di riconoscimento facciale potrebbe non sentirsi libero di agire, cosicché potrebbe cambiare abitudini o comportamenti al fine di sottrarsi al controllo.

2.2.5 Libertà di espressione, di riunione e di associazione

La libertà di espressione, di riunione e di associazione sono diritti fondamentali del cittadino, riconosciuti dalla maggior parte degli ordinamenti del mondo, e in particolar modo costituiscono i capisaldi del rispetto della dignità e della vita dell'individuo in UE e negli USA.

Anche alcuni regimi che si proclamano democratici si sono professati protettori di tali diritti, ma nei fatti ciò non è riscontrabile: emblematici sono i casi di Cina e Russia, che hanno applicato un uso massivo di TRF, al fine di controllare i rivoltosi nella manifestazioni, per ragioni di sicurezza. Si pone dunque un interrogativo: qual è il giusto equilibrio tra sicurezza e libertà negli spazi pubblici?

L'ordinamento statunitense protegge l'anonimato in pubblico: vi è una forte consapevolezza del fatto che l'uso di TRF negli spazi pubblici possa comportare un'interferenza con tali diritti fondamentali, così come disciplinati dal Primo Emendamento. Infatti, in USA il discorso anonimo è protetto, così come lo sono i registri elettorali e gli elenchi di appartenenza alle organizzazioni. In generale l'ordinamento cerca di preservare la maggior parte della privacy di ciascuno.[75][76]

L'ordinamento UE ugualmente protegge tali diritti, sia nella Carta dei diritti fondamentali dell'Unione Europea che nella CEDU. La libertà di espressione è disciplinata all'art. 11 della Carta e all'art 10 della CEDU: è un diritto che appartiene a ciascun individuo in quanto tale, che comprende la libertà di opinione e di ricevere o comunicare informazioni e idee, senza subire ingerenze da parte delle pubbliche autorità. Le libertà di associazione e di riunione sono protette dall'art. 12 della Carta e dall'art. 11 della CEDU: le limitazioni sono ammissibili solo per la salvaguardia di interessi superiori individuati dalla legge, quali per esempio la sicurezza nazionale, pubblica o la prevenzione del crimine.

[75] Reidenberg, «Privacy in Public».

[76] Slobogin, «Public Privacy: Camera Surveillance of Public Places And The Right to Anonymity».

Già nel 2013, il gruppo di lavoro "Articolo 29" ha evidenziato i pericoli connessi all'uso di tali dispositivi in pubblico: emerge il rischio che i soggetti si sentano influenzati nel loro comportamento, dal momento che possono essere localizzati e individuati in ogni momento. Il venir meno della tutela può comportare l'affievolirsi della democrazia partecipativa, interferendo con libertà di riunione e di associazione: le persone si sentono meno libere di agire negli spazi pubblici.[77]

2.2.6 Diritto ad una buona amministrazione

L'ordinamento UE ha elaborato il diritto ad una buona amministrazione. È disciplinato all'art. 41 della Carta dei diritti fondamentali dell'Unione Europea, vincolante per tutti gli stati membri, il quale sancisce che ciascuno ha diritto al trattamento imparziale ed equo delle questioni che lo riguardano, entro un termine ragionevole dalle autorità pubbliche. Tale diritto comprende il diritto di essere ascoltati, prima dell'emissione di un provvedimento a proprio carico, il diritto di ogni persona di accedere al fascicolo che la riguarda, nel rispetto dei legittimi interessi della riservatezza e del segreto professionale e commerciale, e l'obbligo di motivazione per l'amministrazione. Racchiude inoltre il diritto al risarcimento da parte dell'UE dei danni cagionati dalle sue istituzioni o dai suoi agenti nell'esercizio delle loro funzioni.

Tale diritto può venir violato dall'uso di TRF per una mancanza di motivazione nella perquisizione o nell'arresto, fondati sulla corrispondenza del riconoscimento facciale. O ancora il fatto che un soggetto possa accedere ai propri dati necessita che questi abbia la consapevolezza che i propri dati siano stati registrati e conservati. In tal senso l'art. 41 deve essere letto in combinato disposto con l'art. 8 della Carta dei diritti fondamentali, che prevede delle regole nella trattazione dei dati personali: il diritto di accesso ai dati personali e quello di richiedere la rettifica o la cancellazione può essere limitato per evitare di ostacolare indagini, inchieste o procedure ufficiali o legali, di pregiudicare la prevenzione, l'individuazione, l'indagine o il perseguimento

[77] Gruppo di lavoro Articolo 29, «Parere 3/2012 sugli sviluppi nelle tecnologie biometriche».

di reati o l'esecuzione di sanzioni penali, proteggere la sicurezza pubblica o nazionale e proteggere diritti e libertà degli altri.[78]

Ciò che emerge è che manca una consapevolezza di come esercitare il diritto di accesso ai propri dati e la conseguente eliminazione, compresi i dati biometrici.

Al fine di garantire tale diritto una soluzione potrebbe consistere nel prevedere organi controllori, che vadano a garantire prima e dopo l'uso delle tecnologie di riconoscimento facciale, se le persone abbiano effettivamente accesso ai rimedi previsti.

2.2.7 Diritto ad un effettivo ricorso

L'art. 47 della Carta dei diritti fondamentali e l'art. 13 della CEDU sanciscono il diritto ad un ricorso effettivo dinnanzi a un tribunale, compreso il diritto ad un processo equo: i soggetti possono impugnare un provvedimento, adottato da un'autorità, che viola un proprio diritto, comprese le misure assunte sfruttando tecnologie di riconoscimento facciale. È fondamentale che il soggetto sia consapevole del fatto che i suoi dati sono stati acquisiti mediante l'uso di TRF: le autorità, nel momento in cui adottando sistemi che vanno a violare diritti quali la libertà personale o la protezione dei dati per la tutela di interessi superiori, sono tenute a darne comunicazione all'interessato nel momento in cui queste libertà non interferiscono più con le attività di indagine. La notifica di ciò, secondo la Corte di Giustizia dell'UE, è necessaria per consentire alle persone di poter presentare ricorso alle autorità competenti.[79]

Tale diritto è previsto anche in merito alle decisioni che il responsabile del trattamento assume, al fine di permettere al soggetto, i cui dati sono stati trattati, di contestare il motivo per cui la sua immagine è stata usata, o perché è stata ottenuta senza il suo consenso. Ciò permette inoltre di chiedere un risarcimento dei danni nel

[78] «Facial recognition technology: fundamental rights considerations in the context of law enforcement».

[79] Consiglio d'Europa, «Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights» (Strasburgo, 14 maggio 2019), https://www.coe.int/en/web/commissioner/view/-/asset_publisher/ugj3i6qSEkhZ/content/unboxing-artificial-intelligence-10-steps-to-protect-human-rights.

caso in cui siano sorte delle conseguenze negative dalla corrispondenza errata con un'immagine presente nel database.[80]

2.3 Problemi legati alle bias del riconoscimento facciale

I sistemi di riconoscimento facciale, seppur sempre più efficienti e precisi, non risultano ancora sistemi perfetti. Questa mancanza di perfezione emerge in modo lapalissiano nel momento in cui l'algoritmo vada a generare falsi-positivi o falsi-negativi. Questo accade a causa della presenza di *bias*, che creano discriminazioni sistematiche e ingiuste di determinati individui o gruppi in favore di altro: ciò emerge in modo ricorrente con persone con un colore della pelle più scura e con persone di sesso femminile.

Tale problematicità nasce in corrispondenza con la nascita delle immagini: è con lo sviluppo della fotografia che le persone nere iniziano a vivere tale tipologia di discriminazione, in quanto le tecniche di sviluppo delle pellicole si stavano concentrando sul perfezionamento delle tonalità di pelli "caucasiche". Dunque, le immagini erano più adatte a rappresentare le persone con un colore di pelle più chiara. Le aziende Kodak e Fuji possedevano pellicole che non erano in grado di distinguere le diverse gradazioni di pelle non bianca.[81]

Seppur si è realizzato il passaggio a tecnologie fotografiche digitali, che ha permesso un'evoluzione atta a cogliere le diverse tonalità di pelle e i diversi lineamenti, tali *bias* non sono stati del tutto eliminati: emblematico è il caso di una blogger asioamericana, che dopo aver acquistato una fotocamera, dotata di un sistema di riconoscimento facciale, si rese conto che tale sistema non riconosceva la forma allungata degli occhi, dal momento che il dispositivo ad ogni foto chiedeva "*Did someone blink?"*. La donna denunciò la vicenda sul suo blog personale. Si assiste così allo sviluppo di tecnologie che sono più precise nell'individuare i volti delle persone

[80] «Facial recognition technology: fundamental rights considerations in the context of law enforcement».

[81] Lorna Roth, «Looking at Shirley, the Ultimate Norm: Colour Balance, Image Technologies, and Cognitive Equity», *Canadian Journal of Communication* 34 (29 marzo 2009), https://doi.org/10.22230/cjc.2009v34n1a2196; Sarah Lewis, «The Racial Bias Built Into Photography», *The New York Times*, 25 aprile 2019, par. Lens, https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html.

con una pelle più chiara, piuttosto che i c.d. BAME (Black, Asian e minority ethnic).[8283]

I *bias* quindi possono avere origini nel momento della realizzazione dell'algoritmo, in base alle scelte effettuate nella costruzione del modello o delle variabili prese in considerazione: possono riferirsi dunque alla fonte dei dati, si parla di "*bias* di selezione", oppure alla persona che ha la responsabilità di analizzare le informazioni, "*bias* di conferma". Si creano così discriminazione dirette, che sono dipese dall'uso di *labels* come "razza", "etnia", "genere", volte a categorizzare e consentire agli algoritmi di distinguerli, ma che nella loro scelta si rivelano alcune volte generatori di disuguaglianze: è ciò che si è verificato con i grandi dataset, dove si è riscontrata una criticità dell'algoritmo nella lettura del colore della pelle o nell'individuazione del genere.[84]

I processi di *machine learning* possono minare la neutralità che dovrebbe caratterizzare l'intelligenza artificiale: ciò che rimane è la semplice apparenza. Ad influire possono essere plurime ragioni: innanzitutto i pregiudizi del progettista possono condizionare l'impostazione dell'algoritmo, per esempio mediante l'esclusione o l'inclusione di "etichette" che si riferiscono ad una categoria protetta; o ancora il set di dati usato per il training dell'algoritmo può essere influenzato dai pregiudizi di colui che li trasmette oppure i dati possono essere stati raccolti in modo che diano una visione distorta; infine ad incidere sulla creazione di distorsioni può essere un processo autonomo del sistema di *machine learning* che individua caratteristiche come proprie di determinate categorie protette. [85]

Nel 2018 Joy Buolamwini, ricercatrice nel gruppo Civic Media del MIT Media Lab, e Timnit Gebru, sua collaboratrice, hanno elaborato uno studio su tre programmi

[82] Gwen Sharp, «Nikon Camera Says Asians: People Are Always Blinking», *TheSociety Pages* (blog), 29 maggio 2019, https://thesocietypages.org/socimages/2009/05/29/nikon-camera-says-asians-are-always-blinking/.

[83] David Leslie, «Understanding bias in facial recognition technologies: an explainer», *The Alan Turing Institute*, 2020, https://doi.org/10.5281/zenodo.4050457.

[84] Consultative Commitee of the convention 108, «Report on Artificial Intelligence» (Council of Europe, 25 gennaio 2019), https://www.researchgate.net/publication/330910567_Consultative_Committee_of_the_Convention_for_the_Protection_of_Individuals_with_Regard_to_Automatic_Processing_of_Personal_Data_Convention_108_Report_on_Artificial_Intelligence_Artificial_Intelligence.

[85] Paolo Zuddas, «Intelligenza artificiale e discriminazioni» (Consulta Online - Liber Amicorum per Paquale Costanzo, 16 marzo 2020), https://www.giurcost.org/.

che sfruttavano TRF: IBM, Microsoft e Face++.[86] Ciò che è emerso dalla ricerca è che i programmi producevano un tasso d'errore differenziato a seconda che il soggetto, individuato dal dispositivo, fosse maschio o femmina e avesse la pelle più chiara o più scura. Il peggior risultato si otteneva nel caso in cui ad essere riprese fossero le donne con pelle scura, tanto che i tassi di errore in questo caso hanno rilevato che con due dei sistemi analizzati fossero 46.5% e 46.8%: praticamente le tecnologie avrebbero potuto funzionare in modo casuale. Un'indagine condotta recentemente dai ricercatori di IBM, ha dimostrato che in otto tra i più diffusi set di dati presi in considerazione, sei detengono un numero maggiore di immagini di uomini e sei sono principalmente composti da immagini di persone con una tonalità di pelle caucasica. [87] Inoltre, in un dataset contenente più di ventimila immagini, è stato riscontrato come il *labes* razza fosse suddivisa in cinque gruppi: bianchi, neri, asiatici, indiani e altri.[88]

L'algoritmo può realizzare anche le c.d. proxy discriminations (per procura), che agiscono in modo indiretto e sono fondate sul modo in cui dati sensibili vengono utilizzati: essi considerano irrilevanti caratteri che formalmente sarebbero neutri. Questo processo si è aggravato con la diffusione del deep learning, dove i modelli algoritmici individuano autonomamente le caratteristiche con cui costruire il modello biometrico.

La presenza di *bias* nell'uso di TRF può dipendere anche dalla qualità dei dati usati per il training dell'apprendimento automatico del sistema: la scelta sul *data set* deve fondarsi sulla consapevolezza del rischio legato alla possibilità di originare decisione algoritmiche discriminatorie. Il Parlamento europeo si è espresso in merito sancendo che "persino i dati di addestramento di elevata qualità possono portare al perpetuarsi della discriminazione e dell'ingiustizia esistenti, qualora non siano utilizzati in modo attento e consapevole; osserva che l'utilizzo di dati di scarsa qualità, obsoleti, incompleti o inesatti, nelle diverse fasi del trattamento dei dati, può portare a

[86] Joy Buolamwini e Timnit Gebru, «Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification», in *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* (Conference on Fairness, Accountability and Transparency, PMLR, 2018), 77–91, https://proceedings.mlr.press/v81/buolamwini18a.html.

[87] Michele Merler et al., «Diversity in Faces» (New York: IBM Research, 10 aprile 2019), https://arxiv.org/abs/1901.10436.

[88] Kate Crawford e Trevor Paglen, «Excavating AI: The Politics of Images in Machine Learning Training Sets», Excavating AI, 19 settembre 2019, https://excavating.ai.

previsioni e valutazioni inadeguate e, a sua volta, a distorsioni, cosa che può in ultima analisi comportare violazioni dei diritti fondamentali delle persone o conclusioni puramente errate ovvero risultati falsi; ritiene pertanto che nell'era dei big data sia importante garantire che gli algoritmi siano addestrati su campioni rappresentativi di dati di elevata qualità, al fine di conseguire la parità statistica; sottolinea che, anche se si utilizzano dati accurati e di alta qualità, l'analisi predittiva basata sull'IA può offrire solo una probabilità statistica; ricorda che, ai sensi del GDPR, il trattamento ulteriore dei dati personali per scopi statistici, compreso l'addestramento dell'IA, può avere come risultato solo dati aggregati che non possono essere riapplicati agli individui".[89] Nell'uso di TRF ciò può dipendere dal fatto che le immagini acquisite siano rilevate in un ambiente controllato o meno; ma ad incidere nella quantità di falsi-positivi possono essere soprattutto il riflesso della luce, l'inclinazione del volto o il movimento dell'immagine.

Ciò che emerge dalla trattazione fin qui riportata sulla presenza di distorsioni nell'uso di sistemi di riconoscimento facciale è ciò che generalmente si realizza è la creazione di discriminazioni indirette piuttosto che dirette: si assiste all'uso di criteri da parte delle TRF che apparentemente sono neutri, ma nella realtà attribuiscono determinati vantaggi a soggetti che rientrano in determinate *labels*.

Fondamentale in tali casi è la previsione di una tutela per coloro che vengono colpiti da discriminazioni, la quale però risulta tutt'altro che di facile accesso. Il soggetto che voglia dimostrare di essere stato colpito dal modello algoritmico di un dispositivo di AI, che produce effetti discriminatori dovrà sostenere una probatio diabolica: è a suo carico l'onere della prova. Chiaramente dimostrare quanto lamentato appare quasi impossibile, dal momento che dovrà accedere alla *black box* di tali sistemi per far emergere il comportamento esterno.[90]

L'Unione Europea ha cercato di colmare questa carenza di tutela, evitando l'uso di un approccio rimediale: ha elaborato un sistema a monte, che imponga al titolare del trattamento di garantire il "principio di esattezza" dei dati, che sulla correlazione che vi è tra qualità dei dati e finalità per le quali vengono trattati. Ciò permette così la

[89] Parlamento Europeo, «Una politica industriale europea globale in materia di robotica e intelligenza artificiale», Gazzetta ufficiale dell'Unione europea, 12 febbraio 2019, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52019IP0081.

[90] Mobilio, *Tecnologie di riconoscimento facciale p. 223-229.*

possibilità di verificare la presenza di distorsioni. Persiste comunque la possibilità del soggetto leso dai *bias* di AI di esercitare il suo diritto alla conoscibilità della sistema.

Emerge chiaramente come i sistemi di AI, e in particolar modo le TRF, non siano neutrali: i sistemi di AI, intesi come *black box*, il cui funzionamento è imperscrutabile sia per chi si accinge ad usarlo, ma anche per lo stesso progettista, impediscono di verificare se siano presenti delle distorsioni nell'algoritmo. Alcuni studiosi, infatti, invitano alla costruzione di tecnologie che possano decodificare le attività delle *black box*, al fine di salvaguardare autonomia e consapevolezza umana. Sarebbe inoltre necessario il coinvolgimento della popolazione nella realizzazione e nel perfezionamento dell'algoritmo.[91]

2.4 La profilazione

L'utilizzo di tecnologie di riconoscimento facciale, combinato con il fenomeno della profilazione, può rendere sempre più labile il confine tra dimensione pubblica e dimensione privata.

La profilazione dati è definita dal GDPR all'art. 4 come "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica". L'Unione Europea inoltre vieta all'art. 22 GDPR la profilazione automatizzata, salvo il caso in cui non siano previste delle eccezioni per interessi superiori.

La profilazione si compone di sei fasi: la raccolta dei dati, la preparazione dei dati per l'utilizzo, il data mining, l'esame e l'interpretazione dei dati, il follow-up (verifica e correzione) e l'applicazione del profilo. La profilazione sfrutta la propensione delle *big data analytics* e degli algoritmi di *machine learning* ad elaborare dati in forma aggregata. Le informazioni delle persone vengono raccolte nei più ampi metodi: navigando nel web, mediante l'uso di app e in generale attraverso l'uso dei dispositivi

[91] Massimo Airoldi e Daniele Gambetta, «Sul mito della neutralità algoritmica», *The Lab's Quarterly*, n. 4 (2018): 25 s., https://www.researchgate.net/publication/332254603_Sul_mito_della_neutralita_algoritmica.

connessi all'*Internet of Things*.[92] Dunque, una volta collezionati, tali dati vengono raggruppati (*clustered*) in profili sulla base di singoli attributi della persona, come per esempio il comportamento: le persone accumunate dagli stessi aspetti saranno associate allo stesso profilo. L'appartenenza ad uno di questi fa sì che si possano attribuire anche altre caratteristiche tipiche di quel profilo, secondo uno studio probabilistico.

La collezione di dati da parte di sistemi di riconoscimento facciale può comportare dei vantaggi economici: i profili vengono usati per campagne di *microtargeting*, promuovendo annunci personalizzati per i consumatori sulla base del proprio profilo. Uno studio del 2019 ha dimostrato come la pubblicità digitale abbia superato in termini di diffusione la stampa e la tv: le aziende hanno investito prevalentemente in USA in tali mezzi per la promozione di annunci. Ma la profilazione non è in grado di influenzare solo l'economia. Anche i sistemi democratici possono vedere l'intromissione dell'AI volta a interferire con i normali processi decisionali: emblematico è il caso di Cambridge Analytica, società che ha messo a rischio la libera espressione di voto, sia nelle elezioni presidenziali USA del 2016 che nel referendum per la Brexit, mediante la profilazione di milioni di utenti senza il loro consenso.[93]

Uno degli utilizzi della profilazione più dannosi, per la garanzia dei diritti fondamentali, emerge nel caso in cui questa venga associata all'uso di TRF: la loro combinazione può essere ammessa solo se vengono rispettati i principi di proporzionalità e necessità, come avviene nel caso in cui l'obbiettivo sia la tutela della sicurezza nazionale da attacchi terroristici.

La profilazione dunque, associata alle TRF, permette all'algoritmo di confrontare l'immagine del volto di una persona, catturata in uno spazio pubblico, con le numerose informazioni presenti nel web associate a quel volto, siano esse presenti consapevolmente o non. La combinazione di dati sensibili, che all'occhio umano possono sembrare semplicemente "neutri", può fungere da fondamento per la

[92] Valeria Ferraris, «La profilazione e i suoi rischi», in *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica* (Aracne, 2015), 69–80.

[93] Kurt Wagner, «Digital Advertising in the US Is Finally Bigger than Print and Television», Vox, 20 febbraio 2019, https://www.vox.com/2019/2/20/18232433/digital-advertising-facebook-google-growth-tv-print-emarketer-2019.

creazione di profili, conducendo sempre più il soggetto a perdere la propria privacy e l'anonimato in pubblico.

Uno dei rischi più grandi che può incorrere la società nello sfruttamento di tale meccanismo è la degenerazione in una sorta di sorveglianza costante, resa possibile dalla molteplicità di informazioni personali raccolte in forma automatizzata sulla vita pubblica e privata. È ciò che si è verificato con il discusso *Social Credit System* cinese, un sistema di sorveglianza costante attuato dalle autorità, al fine di orientare il comportamento della popolazione, mediante l'attribuzione di vantaggi e sanzioni dipesi dal punteggio che ciascuno detiene: più alto sarà il punteggio ottenuto, più il soggetto avrà la possibilità di beneficiare di determinati servizi pubblici, come i trasporti pubblici, l'iscrizione all'università, o privati, partecipare a concorsi pubblici, ottenere finanziamenti e altro.[94]

2.5 Il consenso

Il consenso è molto spesso usato dalle autorità e dalle società per giustificare l'utilizzo di tecnologie di riconoscimento facciale.

Nell'era del digitale il consenso risulta essere il fondamento delle relazioni che si instaurano con il mondo del web: social networks, cookies e motori di ricerca.

La questione relativa al consenso si è posta in merito alla funzione di Facebook che suggerisce automaticamente agli utenti le persone da "taggare", qualora queste fossero già state identificate sulla base di un sistema di riconoscimento facciale. Tale funzionalità ha da subito suscitato molte discussioni in UE, in quanto si riteneva che tale funzione violasse il requisito del consenso.

Negli USA la *Federal Trade Commission* ha elaborato le FIPs (*Fair Information Practices*), ossia della norme per il trattamento delle informazioni, che disciplinano anche i modelli "*notice-and-choice*": sono validi se viene dimostrato che il consenso non sia ingannevole o sleale. Ma ciò che emerge è che l'informativa su come verranno trattati i dati personali, è seppellita in una densa politica privacy, che cerca di equiparare il concetto di privacy a quello di controllo, ottenuto mediante l'accettazione dell'informativa.[95]

[94] Mobilio, *Tecnologie di riconoscimento facciale p. 201 ss*.

[95] Hartzog, «Privacy'S Blueprint» p. 58-72.

Ma nell'uso delle TRF ciò che sembra emergere come più lesivo del consenso del soggetto al trattamento dei dati personali, sembra essere l'uso di sistemi passivi di TRF. Il fatto di entrare all'interno di un'area videosorvegliata non implica automaticamente acconsentire a che i dispositivi utilizzino dati personali: infatti il Comitato europeo per la protezione dei dati ha stabilito che affinché ciò possa accadere, è necessario che siano rispettati i parametri previsti all'art. 9 GDPR: i mezzi di rilevamento devono poter essere attivati dall'interessato o sarebbe necessario predisporre una separazione degli ambienti sottoposti a TRF.[96]

L'approccio dell'UE risulta essere più rigoroso di quello adottato dagli USA: nel 2016 è stato emanato il GDPR, che considera privacy e protezione dei dati personali come diritti fondamentali. Il Considerando Sette del GDPR prevede in merito che sia "opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano": questo è effettuato tramite il "consenso informato". Ma nonostante il diverso modo di considerare i diritti emerge come entrambi gli ordinamenti pongano al centro della risoluzione del problema della privacy il consenso.

Un problema in merito alla consapevolezza sul consenso emerge in modo chiaro nel momento in cui al soggetto sia sottoposto un documento sull'informativa al consenso del trattamento dei dati: tali testi generalmente vengono redatti in modo molto complesso, con termini giuridici, che rendono quasi impossibile la comprensione a chi non detiene conoscenze specifiche. A ciò si aggiunge un'ulteriore difficoltà di comprensione nel caso in cui tali dati vengano sfruttati da mezzi informatici automatizzati. Secondo Nancy Kim, infatti, uno dei requisiti per la validità del consenso consta nella conoscenza da parte del soggetto del motivo per cui lo si esprime e la conseguente volontà a darlo: devono essere chiari gli scopi perseguiti dalla tecnologia mediante l'uso dei dati personali di cui si ha acconsentito il trattamento. Ciò che consegue da tale mancanza è l'emersione di un'asimmetria informativa dipesa dall'incapacità del soggetto di prendere consapevolezza su ciò a cui è sottoposto: viene violata dunque la sua libertà di autodeterminazione. Le condizioni presenti in tali informative, dunque, seppur richiedono la manifestazione del consenso, non intendono affermare che questo venga manifestato in modo

[96] Gruppo di lavoto articolo 29, «Linee guida sul consenso ai sensi del regolamento (UE) 2016/679» p. 20 ss., 10 aprile 2018, http://ec.europa.eu/justice/data-protection/index_en.htm.

volontario, questo perché si è in presenza del consenso inconsapevole.[97] Ulteriore requisito per la validità del consenso: i benefici sociali debbono andare a superare i danni sociali.[98]

Ma nonostante l'ampia rilevanza del consenso, questa non può essere considerata assoluta, in quanto si rischierebbe di dare troppa rilevanza a nozioni quali l'autonomia e il controllo, piuttosto che un corretto bilanciamento della privacy, che potrebbe passare in secondo piano con la giustificazione che il soggetto avrebbe acconsentito al trattamento, sebbene egli sia inconsapevole.

Alcune volte può accadere che il consenso alla sottoposizione a TRF venga prestato in modo tutt'altro che volontario: si tratta del caso del consenso forzato. In questa situazione la scelta che si pone di fronte al soggetto consta dell'accoglimento o della perdita di un bene importante, quali il lavoro. Il rischio che si corre è che a subire tali meccanismi siano principalmente le più povere o più deboli socialmente, dal momento che la loro posizione di svantaggio persone li pone in una condizione di accettare tutte le possibili condizioni in un contesto di non piena libertà.

Il consenso nel contesto digitale usato in questo modo viene privato del suo ruolo fondamentale: quella di controllare l'utilizzo dei propri dati personali. Si assiste costantemente allo sfruttamento delle sue patologie ad opera di aziende al fine economico, ma allo stesso tempo anche a continui abusi e furti di dati che stanno facendo diminuire la fiducia nei consumatori nel mondo digitale. [99]

Si può rilevare dunque che il consenso, nell'uso TRF, non riesce a prestare una protezione all'individuo.

2.6 L'importanza del design nell'AI

La progettazione di ogni oggetto che ci circonda influenza il modo con cui lo si percepisce: basti pensare all'uso del simbolo del lucchetto nelle pagine di numerosi

[97] Neil Richards e Woodrow Hartzog, «The Pathologies of Digital Consent», *Washington University Law Review* 96, n. 6 (2019): 1461–1503, https://law.northeastern.edu/faculty/hartzog/.

[98] Woodrow Hartzog e Evan Selinger, «The Inconsentability of Facial Surveillance», *Loyola Law Review* 66 (2019): 101–22, https://law.northeastern.edu/faculty/hartzog/.

[99] Richards e Hartzog, «The Pathologies of Digital Consent».

siti web per indicare che si tratta di un sito sicuro. In questo caso la nostra mente associa in modo automatico tale caratteristiche all'icona sulla sicurezza.

Il design assume una rilevanza particolare nelle tecnologie di AI: contribuisce alla protezione delle privacy e dei dati personali.

Le leggi fino ad ora hanno fallito nel disciplinare il design dei sistemi informatici: ciò ha permesso alle grandi aziende di poter agire in modo indiscriminato, sfruttando i *gap* di progettazione. Nell'era del digitale i dati sono diventati il carburante delle aziende e la presenza di un design efficiente e privo di falle potrebbe essere letale per la loro fortuna economica. Al contrario un "cattivo design" può nascondere le violazioni di privacy e permettere alle aziende di sfruttare in modo indisturbato le enormi quantità di informazioni che costantemente vengono cedute dagli utenti nel web.

Le società non possono essere lasciare libere nella regolamentazione della tecnologia, è necessario l'intervento dei legislatori. Designers e programmatori, infatti, hanno un ruolo molto rilevante perché possono produrre delle implicazioni anche a lungo termine mediante le scelte di progettazione: sarebbe dunque necessario che fossero affiancati anche esperti nel campo in cui tale tecnologia andrà ad essere usata, dal momento che per ogni azione è necessario valutare tutti i costi e i benefici, onde evitare la realizzazione di ingiustizia sociale.[100]

La presenza di un design proattivo può essere molto efficace nel garantire la prevenzione di discriminazioni o lesioni di diritti. Al contrario, se si adotta un design reattivo può accadere che non sempre si riesca ad individuare specificatamente il problema per cui si debba trovare una soluzione. [101]

C'è molta cautela da parte dei legislatori nel regolamentare: vi è la necessità di bilanciare la sicurezza, al fine di prevenire la creazione di falle del sistema che permettono violazioni costanti di privacy, ma allo stesso tempo è fondamentale garantire alle compagnie una libertà d'azione. La previsione di leggi sulla privacy che incidono nel design può cercare di porre rimedio.

[100] Joy Ito, «AI Engineers Must Open Their Designs to Democratic Control», American Civil Liberties Union, 2 aprile 2018, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/ai-engineers-must-open-their-designs-democratic.

[101] Ann Cavoukian, «Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices», 2009, https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

L'approccio statunitense alla regolazione avviene mediante la produzione di norme che vanno a regolare una questione alla volta e che non fanno capo ad un sistema centralizzato. Le FIPs però ignorano il design, non affrontano il problema di come la tecnologia influenzi le persone: disciplinano semplicemente come le informazioni debbano essere collezionate e trattate.[102]

In UE emerge invece un approccio diverso, più ampio, che mira alla protezione dei diritti umani e dei dati personali. La disciplina dei requisiti in materia di protezione dei dati fin dalla progettazione e per impostazione predefinita la si rinviene all'art. 25 del GDPR: si parla di *data protection by design*. L'obbiettivo di tale norma è andare ad imporre, ai responsabili del trattamento di dati, l'obbligo di attuare misure tecniche e organizzative volte a garantire che la vendita di dati rispetti il regolamento sulla protezione. Tale disposizione è concepita in modo molto ambizioso, ma emergono in realtà alcune difficoltà nella sua applicazione, dipese dall'eccessiva vaghezza, dalla mancanza di chiarezza su parametri e metodologie per raggiungere gli scopi e da una mancanza di comunicazione diretta con coloro che realizzano il progetto e il suo sviluppo. A rendere più difficile la sua applicazione contribuisce anche il fatto che ciò può confliggere con numerosi interessi di organizzazioni che hanno grande influenza nel mercato.[103]

Per quanto attiene all'uso di TRF, sfruttare il design per proteggere i dati significa individuare un insieme di principi e diritti che regola la tecnologia. Nel GDPR si riscontra il tentativo di anticipare la protezione ad un momento precedente al realizzarsi della lesione. Deve emergere il rispetto del principio di minimizzazione: secondo quanto disposto dall'art. 5 del GDPR i dati biometrici possono essere conservati fintantoché siano necessari per il perseguimento delle finalità per cui sono stati raccolti; una volta venuta meno la base giuridica è necessario procedere alla cancellazione. Inoltre, è possibile procedere ad una conservazione di dati biometrici in forma pseudonimizzata o criptata; o ancora prevedere che i set di dati siano conservati in dataset centralizzati o su portatili.

[102] Hartzog, «Privacy'S Blueprint» p.56-90.

[103] Lee A. Bygrave, «Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements», *Oslo Law Review* 4, n. 02 (2017): 105–20, https://doi.org/10.18261/issn.2387-3299-2017-02-03.

La comprensibilità del sistema non deve essere sancita solo a livello normativo, deve essere reale ed effettiva: è il linguaggio usato che garantisce l'effettività della comprensione. Ciò permette che il soggetto sia consapevole di essere sottoposto a TRF e di potere esercitare determinati diritti.[104]

Il design è fondamentale anche per la prevenzione delle bias: è sulla base della scelta dell'algoritmo che si possono prevenire distorsioni che conducono a discriminazioni, dal momento che il *machine learning* deve essere progettato senza l'imposizione di *labels* che possono incidere nel trattamento di determinati individui.

Nelle TRF tra si instaura un rapporto di interazione tra "*code and law*": da un lato la legge può vincolare il codice imponendo determinati canoni o valori lungo tutto il procedimento di decisione algoritmica; parallelamente il codice può vincolare la legge influendo sull'attuazione ed effettività come accade sulla base del principio *legal by design*.[105]

I processi decisionali degli algoritmi possono condurre dunque a decisioni automatizzate che incidono nella vita delle persone, interferendo anche con la tradizionale tutela dei diritti fondamentali. In tale contesto si inserisce la nozione *Legal Protection by Design*, secondo cui le norme giuridiche, approvate da un legislatore che rappresenta la volontà popolare, vengono tradotte nelle norme tecnologiche che regolano il processo decisionale dell'algoritmo, al fine di regolamentare anche quella realtà parallela che si crea nel mondo delle tecnologie, dal momento che nell'era digitale si assiste sempre più fortemente ad una perfetta integrazione tra l'ambiente digitale e quello fisico. Il design di una tecnologia può dirsi anche politico, perché dipende dalle norme giuridiche che vengono tradotte in comandi: questi possono influire sui poteri, sulle conoscenze e competenze, ma soprattutto sulla protezione che tali sistemi di AI possono far emergere. È importante, dunque, che la legge preveda dei limiti per tali sistemi. Ma nella traduzione delle leggi in comandi sorge una difficoltà: i due sistemi agiscono in modo diverso, dal momento che la produzione normativa segue, per esempio nei paesi liberal-democratici, un procedimento che è circondato da garanzie, come la legittimazione del soggetto che emana le norme. Inoltre, anche la libertà individuale sembra essere lesa da tali sistemi, nonostante la loro disciplina si fondi su norme giuridiche: le persone si trovano di

[104] Zuddas, «Intelligenza artificiale e discriminazioni».

[105] Mobilio, *Tecnologie di riconoscimento facciale 317-327*.

fronte ad una scelta, tenere o non un determinato comportamento; al contrario la legge appare più flessibile: è possibile anche trasgredirla, può subire interpretazioni differenti.[106]

2.7 L'etica della responsabilità nella costruzione dell'AI

L'etica della responsabilità trova una prima concettualizzazione in Max Weber nel 1961: tale nozione indica come sia necessaria la presenza di cittadini e governanti responsabili, nel senso che ciascuno è in grado di prevedere le conseguenze delle proprie azioni, in quanto l'*agere* non è mai indifferente e la società ha bisogno di essere orientata verso il bene. L'agente responsabile deve rispondere dei danni cagionati dalle sue azioni, nel caso in cui questi siano prevedibili.

Il concetto di responsabilità è stato fatto oggetto di una nuova riconsiderazione ad opera di Hans Jonas. Egli si è reso autore di una massima: "agisci in modo che le conseguenze della tua azione siano compatibili con la permanenza di un'autentica vita umana sulla terra". Tale massima si riferisce all'azione umana, alla sua intelligenza, alla sua capacità di previsione, al suo controllo.

Ma ciò che emerge in modo chiaro, è che nell'era del digitale la responsabilità si addentra in confini molto lontani da quelli in cui Weber aveva delineato il concetto di etica della responsabilità. Gli sviluppi tecnologici hanno contribuito ad una ridistribuzione degli incarichi che vede sempre più protagoniste le macchine: le normali azioni che un tempo erano compiute dall'uomo, attualmente vedono il loro compimento ad opera di tecnologie, sempre più sviluppate e precise, al punto tale da superare le capacità dell'uomo.

In tale scenario sorge un problema in merito alla responsabilità di tali azioni. Ampia rilevanza assumono designers e ingegneri, che nel progettare nuovi sistemi tecnologici non possono non bilanciare anche gli altri interessi della società, dal momento che le scelte da essi operate hanno delle implicazioni a lungo termine.[107]

---

[106] Mireille Hildebrandt, «Saved by Design? The Case of Legal Protection by Design», *Nonoethics* 11 (25 agosto 2017): 307–11, https://doi.org/10.1007/s11569-017-0299-0; Teresa Scantamburlo, Andrew Charlesworth, e Nello Cristianini, «Machine Decisions and Human Consequences», in *Algorithmic Regulation*, 2019, 49–81, https://doi.org/10.1093/oso/9780198838494.003.0003.

[107] Umberto Vincenti, *Introduzione all'etica pubblica: Dispense ad uso degli studenti.* (Edizioni libreria progetto Padova, 2020) p. 63-65.

L'esigenza di regolamentare le pratiche di professionisti sulla tecnologia è così sentita al punto tale che nel 2018 la *Task Force ACM Code* ha elaborato un codice etico, ACM Code of Ethics and Professional Conduct, volto a regolare le azioni di esperti dell'informatica.[108] Inoltre, l'Unione Europea nell'ambito del progetto Horizon 2020, ha promosso due Framework: Responsible Research Innovation (RRI) e Value Sensitive Design (VSD). L'RRI ha l'obbiettivo di promuovere una collaborazione, nell'ambito della ricerca e dell'innovazione, tra i diversi attori della società al fine di rispettare tutti i valori, aspettative e bisogni. [109] Il VSD invece è un approccio che considera i principi e i valori degli esseri umani che devono essere applicati quando si sta progettando una piattaforma tecnologica. L'obbiettivo dell'UE è dunque quello di promuovere una stretta interrelazione tra designer, utente e policy makers.[110]

Il design di ogni sistema informatico deve essere ispirato a principi e valori che devono rispecchiare quelli condivisi dalla società: non è possibile che questi vengano valutati da tecnici o operatori economici, privi di alcuna conoscenza in merito alle implicazioni delle loro azioni, perché ciò comporterebbe il rischio che sistemi di AI siano disciplinati da *self-regulation*.

Al fine di garantire un design efficiente, ma allo stesso tempo che non vada a violare i diritti fondamentali, una soluzione che può figurarsi è quella delineata anche dalla Commissione Europea nei Framework elaborati nell'ambito del progetto Horizon 2020 che vede una collaborazione tra informatici da una parte e dall'altra tra legislatori e decisori politici: i primi hanno il dovere di realizzare modelli algoritmici che incorporino valori e che possano essere oggetto di verifica in un momento successivo; i secondi invece hanno il dovere di delineare standard da sottoporre a scienziati, al fine di porre dei limiti e tracciare i confini entro cui possono elaborare nuove tecnologie.[111]

Oltre a tali approcci elaborati dalle istituzioni, un'ulteriore accortezza da adottare per arginare i rischi che intercorrono nella progettazione, si basa sulla predisposizione di una formazione per informatici e scienziati al fine di far comprendere loro il valore

[108] «ACM Code of Ethics and Professional Conduct», 2018, https://www.acm.org/code-of-ethics.

[109] «Responsible Research & Innovation», Horizon 2020 - European Commission, 2020, https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation.

[110] «About VSD», *VSD Lab* (blog), s.d., https://vsdesign.org/vsd/.

[111] Joanna Huey et al., «Accountable Algorithms», *University of Pennsylvania Law Review* 165 (2017): 633 ss., https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/.

dei principi, quali la "*privacy by design*": si parla in tal caso di "*tutela by education*". Una piena consapevolezza delle implicazione che tali tecnologie comportano risulta fondamentale. Assumono rilevanza il ruolo di formatori nelle associazioni professionali o accademiche: le loro azioni di tecnici devono ispirarsi costantemente a valori quali la dignità e la libertà delle persone. Nel momento in cui realizzano un nuovo algoritmo, gli scienziati devono dunque essere in grado di prevedere quali sono le possibili applicazione che possano venir compiute. A questo fine, a seguito della conferenza *Neural Information Processing Systems* del 2020, è stato stabilito che gli scienziati debbano predisporre una dichiarazione che affronti le preoccupazioni etiche e i potenziali esiti negativi del loro lavoro.[112]

Uno sondaggio effettuato da Richard Van Noorden su *Nature* ha evidenziato come su 480 ricercatori, molti siano consapevoli delle problematicità etiche che affliggono i dispositivi di AI e in particolar modo le TRF. Emerge infatti come molti scienziati stiano invitando i colleghi a non lavorare con società che non predispongano degli appositi accorgimenti in campo etico.[113]

[112] Andrea Simoncini e Samir Suweis, «Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale», *Rivista di filosofia del diritto, Journal of Legal Philosophy*, gennaio 2019, 87–106, https://www.rivisteweb.it/doi/10.4477/93368.

[113] Richard Van Noorden, «The Ethical Questions That Haunt Facial-Recognition Research», *Nature* 587, n. 7834 (18 Novembre 2020): 354–58, https://doi.org/10.1038/d41586-020-03187-3.

3. UNIONE EUROPEA

3.1 Libro bianco sull'AI e proposta di regolamento del Parlamento Europeo

"Dobbiamo intensificare gli sforzi per definire la nostra trasformazione digitale secondo le nostre norme e i nostri valori" è quanto sostiene Ursula von der Leyen nel discorso tenutosi il 15 settembre 2021 di fronte al Parlamento europeo, in merito allo stato dell'Unione.[114] La Presidente della Commissione, nel delineare le priorità che richiedono l'attenzione di una regolamentazione da parte dell'Unione, evidenzia come il digitale, nella sua totalità, abbia assunto un ruolo decisivo nella vita delle persone, tale da richiedere un posto centrale nell'agenda dei diversi organismi istituzionali europei. È noto, infatti, come l'UE negli ultimi anni, abbia adottato una strategia volta a garantire lo sviluppo e l'innovazione della tecnologia digitale, con l'obbiettivo di creare un complesso di norme prodotte da una visione lungimirante e da una competenza profonda, che non frena l'innovazione, ma la guida: percorrendo tale via si potrà ottenere da un lato il rilancio dell'industria digitale europea e dall'altro il rispetto dei diritti umani.[115]

Il percorso di normazione che si prefigge lo scopo di aumentare gli investimenti nell'ambito delle nuove tecnologie digitali può dirsi iniziato, in modo graduale, già a partire dagli anni passati, dove si è assistito all'emanazione di una serie di atti da parte della comunità, con l'obbiettivo di armonizzare le legislazioni nel settore dello sviluppo tecnologico. Tra questi merita particolare menzione il General Data Protection Regulation (GDPR)[116], adottato il 27 aprile 2016 e attuato due anni dopo, dal 25 maggio 2018. Specificamente in riferimento ai sistemi di riconoscimento facciale, il regolamento europeo per primo disciplina tali strumenti, prevedendone l'utilizzo limitatamente ai contesti definiti "critici" sotto il profilo della sicurezza, quali gli aeroporti. Nel 2021 è stato pubblicato infatti un rapporto di *Airports Council International World* (ACI) sugli investimenti effettuati dagli aeroporti, che rivela come questi abbiano speso buona parte dei ricavi in tecnologia: tra queste emerge

[114] «Discorso sullo stato dell'Unione della Presidente von der Leyen», Text, European Commission - European Commission, 15 settembre 2021, https://ec.europa.eu/commission/presscorner/detail/it/SPEECH_21_4701.

[115] Luca De Biase, «Il difficile equilibrio tra innovazione e tutela dei diritti», *ECONOMIA E POLITICA INTERNAZIONALE*, 22 aprile 2021, https://mydesk24.ilsole24ore.com/crui.

[116] «Regolamento UE 2016/679, GDPR, General Data Protection Regulation» (2016).

anche la TRF, la quale risulta garantire maggiore sicurezza, in un tempo in cui la pandemia, che dall'inizio 2020 sta influenzando la vita di ciascuno di noi, impone alla persone di evitare qualsiasi contatto per limitare i danni che possono essere causati dalla diffusione del virus.[117]

L'art. 9 paragrafo 1 del GDPR prevede un divieto generale al trattamento di dati personali, sancendo: "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", con ciò riferendosi dunque anche all'uso della tecnologia in questione. Nonostante tale divieto sia chiaro ed esplicito, il paragrafo 2 del presente articolo prevede delle eccezioni in alcuni casi specifici: l'utilizzo di dati biometrici è ammesso nel caso in cui sia necessario per ragioni in ambito lavorativo o nell'ambito della sicurezza sociale e collettiva; se necessario per la protezione di un interesse vitale dell'interessato o di altra persona; se necessario in un procedimento giudiziario; se vengono rilevati particolari motivi di interesse pubblico o per motivi di sicurezza sanitaria, controllo e prevenzione di malattie trasmissibili e per la tutela di gravi minacce per la salute delle persone fisiche.[118]

Successivamente, nel febbraio 2020, la Commissione Europea ha pubblicato il Libro Bianco sull'intelligenza artificiale: un documento in cui l'Unione Europea delinea come l'AI stia sempre più condizionando le vite delle persone, con effetti positivi, quali l'aumento dell'efficienza dell'agricoltura, della produzione o dell'assistenza sanitaria, ma anche comportando rischi potenziali, quali meccanismi decisionali opachi, discriminazioni basate sul genere o intrusioni che comportano violazioni di diritti fondamentali. L'obbiettivo della Commissione è presentare un sistema normativo europeo che possa affrontare in modo univoco le nuove sfide che stanno emergendo con sviluppi tecnologici, che tenga conto contemporaneamente dei valori fondamentali, quali la dignità umana e la tutela della privacy, e che rispetti il principio di precauzione, adottato dalle autorità come metodo di valutazione, calcolo,

[117] Airports Council International, «Airport Economics Report 2021 - A comprehensive view of the industry's financial performance», 2021.

[118] «Art. 9 Regolamento UE 2016/679, GDPR» (2016).

gestione e comunicazione dei rischi che la scienza non è in grado di rilevare pienamente.[119]

Il progetto che le istituzioni europee intendono realizzare si compone di due elementi fondamentali:

1. Incentivare gli investimenti nella ricerca, innovazione e diffusione di AI, coinvolgendo anche il settore della piccola-media impresa, sia a livello nazionale che europeo;
2. Diffondere e implementare la fiducia dei cittadini nell'AI, riducendo le asimmetrie informative, in modo che possano sentirsi sicuri nell'adottare o nell'essere sottoposti a tali sistemi, grazie alla presenza di un quadro normativo chiaro e uniforme in tutti i paesi, tale da rendere le innovazioni utili e non solo dannose.

Inoltre, la Commissione Europea sancisce la necessità di una definizione di Artificial Intelligence, che tenga conto delle attuali caratteristiche di tali strumenti, ma che contemporaneamente sia in grado di adattarsi agli sviluppi successivi.

La regolazione dell'AI che il Libro Bianco delinea nel progetto presentato adotta un *risk-based approach*, con l'obbiettivo di costruire un sistema normativo che possa rispettare il principio di precauzione e di proporzionalità. La Commissione evidenzia in tale Report che i sistemi di AI sono classificati in base al rischio: questo viene calcolato tenendo conto degli interessi in gioco, del settore considerato e dei relativi rischi. Si parla di AI ad *high-risk* nel caso in cui questa sia utilizzata in ambiti in cui si possano prevedere rischi significativi e tenendo conto anche del modo in cui è usata. Può accadere però, secondo quanto riporta la Commissione presieduta da Ursula Von Der Leyen, che un sistema di AI sia considerato ad alto rischio in sé, a prescindere dalla sussistenza di tali due condizioni: è il caso di tecnologie di intelligenza artificiale usate nei processi di selezione del personale e nelle situazioni relative ai lavoratori e nel caso dell'uso di tecnologie di identificazione biometrica remota e sorveglianza intrusiva.[120]

[119] Mobilio, *Tecnologie di riconoscimento facciale p. 291-301.*

[120] «Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia» (Commissione europea, 19 febbraio 2020), 4; «Opinion 4/2020 on the European Commission's White Papaer on Artificial Intelligence - A European approach to excellence and trust, cit. p. 27» (European Data Protection Supervisor, 29 giugno 2020).

In merito, è intervenuto anche il Comitato della Commissione 108 del Consiglio d'Europa, il quale, in un documento pubblicato il 28 gennaio 2021, *Linee guida sul riconoscimento facciale*, ha sottolineato l'importanza di una regolamentazione del digitale, in riferimento alle TRF. "These guidelines provide a set of reference measures that governments, facial recognition developers, manufacturers, service providers and entities using facial recognition technologies should follow and apply to ensure that they do not adversely affect the human dignity, human rights and fundamental freedoms of any person, including the right to protection of personal data" si legge nel documento pubblicato dalla Convenzione 108, in cui viene in rilievo il contrasto tra l'impiego degli strumenti in questione e i diritti fondamentali.[121] Di centrale importanza risulta l'affidabilità degli strumenti, che dipende dall'effettività dell'algoritmo impiegato e da altri fattori quali la qualità delle telecamere impiegate, l'assenza di falsi positivi e falsi negativi. A ciò si aggiungono la sicurezza dei dati impiegati, che devono essere protetti dalla divulgazione e dai possibili abusi che possono essere perpetrati, e la consapevolezza dell'utilizzo dei dati e la loro comprensione da parte degli interessati che deve essere alimentata mediante l'educazione.[122] Infine, è auspicabile l'individuazione di un framework etico, con la conseguente costituzione di comitati etici indipendenti da consultare, ogni qualvolta la questione relativa alla tutela dei diritti dell'uomo viene in rilievo.[123]

A conclusione delle diverse regolamentazioni ed interventi proposti dalla comunità, è nel programma, "un'Unione più ambiziosa"[124], delineato dalla Presidente della Commissione 2019-2024, che si inserisce la proposta di regolamento 2021/0106 del Parlamento Europeo e del Consiglio del 21 aprile 2021, che stabilisce "regole armonizzate sull'intelligenza artificiale" e modifica alcuni atti legislativi dell'Unione Europea[125]. Tale disegno di legge impone a coloro che utilizzano sistemi di AI nel

[121] Convention 108, «Guidelines on Facial Recognition Directorate General - Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data», 28 febbraio 2021, 3.

[122] Convention 108, 5–10.

[123] Convention 108, 14.

[124] Ursula von der Leyen, «Un'Unione più ambiziosa - Il mio programma per l'Europa», 2019.

[125] «Proposta di regolamento UE 2021/0106, del Parlamento Europeo e del Consiglio del 21 aprile 2021, che stabilisce "regole armonizzate sull'intelligenza artificiale" e modifica alcuni atti legislativi dell'Unione Europea» (2021).

mercato europeo oneri di conformità ai valori dell'UE e alla normativa in ambito di diritti fondamentali, nel rispetto del principio di proporzionalità e di precauzione. Un ulteriore obbiettivo riscontrabile nel testo del regolamento emerge nelle norme volte a migliorare la *governance* e a garantire l'efficace attuazione di tali diritti nel contesto dell'AI. Il regolamento inoltre prevede investimenti e innovazioni per la creazione di un mercato unico per sistemi di AI legittimi e affidabili, che forniscono certezza giuridica sull'AI e sulle sue applicazioni. Quindi è chiaro come il regolamento voglia eliminare l'eterogeneità normativa a livello nazionale che può provocare una frammentazione del mercato interno, a favore di un'armonizzazione della regolamentazione dello sviluppo, della commercializzazione e dell'uso dell'AI. Il regolamento non intende dunque esaurire i profili di interesse giuridico dell'AI, ma piuttosto si inserisce in un quadro normativo più ampio, definendo un decalogo di divieti e obblighi modulati e scalari sulla base del rischio che il sistema solleva rispetto ai valori dell'Unione.[126]

Con il presente regolamento l'UE classifica le diverse tecnologie di intelligenza artificiale sulla base del livello di rischio, seguendo il *risk-based approach* presente nel Libro Bianco: le tecnologie vengono classificate sulla base del fatto che il loro utilizzo possa causare un rischio inaccettabile, un rischio alto o un rischio basso o minimo. Per quanto riguarda quest'ultimi, la disposizione normativa prevede che la loro regolamentazione venga lasciata libera all'autodeterminazione del mercato, nel rispetto di limiti, quali l'equità e la correttezza.

La proposta di regolamento disciplina al titolo III i sistemi ad alto rischio: l'art. 6 paragrafo 1[127] stabilisce due condizioni che devono essere soddisfatte affinché si possa parlare di sistemi ad alto rischio:

1. Il sistema di AI è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'unione.
2. Il prodotto, il cui componente di sicurezza è il sistema di AI, o il sistema di AI stesso in quanto prodotto è soggetto ad una valutazione della conformità

[126] «Relazione sulla proposta di regolamento UE 2021/0106», 21 aprile 2021.

[127] Art. 6 paragrafo 1 Proposta di regolamento UE 2021/0106, del Parlamento Europeo e del Consiglio del 21 aprile 2021, che stabilisce "regole armonizzate sull'intelligenza artificiale" e modifica alcuni atti legislativi dell'Unione Europea.

da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione.

Il titolo II disciplina invece le pratiche di intelligenza artificiale vietate, in quanto il loro utilizzo può essere causa di rischi inaccettabili rispetto ai valori dell'UE. L'art. 5[128] stabilisce il divieto per: quei sistemi che utilizzano tecniche subliminali in grado di manipolare il comportamento di una persona con probabili conseguenze fisiche o psicologiche a danno di quel soggetto o di altri; i sistemi che sfruttano le debolezze di un gruppo specifico di soggetti vulnerabili come l'età, la disabilità fisica o mentale al fine di manipolare il comportamento di un soggetto appartenente a tale gruppo, con probabili conseguenze fisiche o psicologiche a danno di quel soggetto o di altri soggetti; quelli utilizzati dalle pubbliche autorità o per conto di pubbliche autorità al fine di valutare e classificare l'affidabilità delle persone fisiche sulla base del loro comportamento sociale; o ancora quelli che consentono l'identificazione biometrica a distanza "in tempo reale" a fine di contrasto a meno che l'uso di questi sistemi non sia strettamente necessario per determinati obbiettivi, quali la ricerca mirata di potenziali vittime da reato, compresi minori scomparsi; prevenzione di una minaccia specifica, sostanziale e imminente per la vita e l'incolumità fisica dei soggetti o di un attacco terroristico; il rilevamento, l'identificazione o l'azione penale di un autore o sospettato di reato.[129]

Tuttavia, il regolamento non si limita semplicemente a delineare cosa sia vietato e cosa no, ma al fine di una maggior comprensione e un'unanime interpretazione che eviti contrasti sul significato delle parole utilizzate, come spesso accade, fornisce all'art. 3 una serie di definizioni relative agli strumenti dell'Artificial Intelligence. Stabilisce infatti il significato di sistema di identificazione biometrica remota: si tratta di "sistemi di AI finalizzati all'identificazione a distanza di persone fisiche mediante il confronto di dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento, e senza che l'utente sappia se la persona sarà presente e può essere identificata". Definisce inoltre cosa debba intendersi per sistemi di identificazione biometrica remota in tempo reale: si tratta di quei sistemi in cui l'identificazione

[128] Art. 5 Proposta di regolamento UE 2021/0106, del Parlamento Europeo e del Consiglio del 21 aprile 2021, che stabilisce "regole armonizzate sull'intelligenza artificiale" e modifica alcuni atti legislativi dell'Unione Europea.

[129] Valeria Falce, «Intelligenza artificiale, regole a tenuta dei valori UE», *NORME E TRIBUTI*, 6 ottobre 2021, 36, https://mydesk24.ilsole24ore.com/crui.

avviene senza ritardi significativi, con esso intendendo anche il caso quelle che avvengono con brevi ritardi.[130]

Dunque, ciò che l'Unione sembra voler costruire è un sistema che prevenga una sorveglianza di massa che monitora costantemente i comportamenti delle persone e che limita i diritti inviolabili tanto combattuti nel corso dei secoli. Piuttosto appare chiara l'intenzione di impiegare la tecnologia in settori strategici, per trarre quei benefici che le capacità umane non sono in grado di offrire, con l'obbiettivo di portare vantaggi alla società, quali ad esempio la sicurezza nelle città, la prevenzione di attentati terroristici e l'individuazione di soggetti pericolosi.

In merito alla proposta di regolamento si sono espressi anche l'European Data Protection Board (EDPB) e l'European Data Protection Supervisor (EDPS), i quali nel parere congiunto 5/2021 del 18 giugno 2021 hanno espresso dubbi in merito al largo impiego delle tecnologie di AI. Perplessità sono inoltre emerse in relazione alla regolamentazione dei sistemi di riconoscimento facciale, per i quali l'opinione espressa mira ad un divieto dell'impiego di strumenti che sfruttino riconoscimento automatico delle caratteristiche umane in spazi accessibili al pubblico, come il volto, l'andatura, ecc. a cui si connette un ulteriore divieto per le pratiche di categorizzazione delle persone in insiemi, che si fondano su etnia, dati biometrici, genere, orientamento politico, sessuale o per altri per cui la discriminazione è vietata ai sensi dell'art. 21 della Carta dei diritti fondamentali dell'Unione Europea[131]. Secondo le due autorità sono inoltre da escludere quelle tecnologie che possono rilevare lo stato emotivo di una persona. Al fine di evitare una violazione dei diritti fondamentali e dei valori europei, tali tecnologie, secondo l'EDPB e l'EDPS dovrebbero essere inserite nell'elenco presente all'art. 5, che stabilisce quali siano le pratiche vietate.[132]

[130] Art. 3 Proposta di regolamento UE 2021/0106, del Parlamento Europeo e del Consiglio del 21 aprile 2021, che stabilisce "regole armonizzate sull'intelligenza artificiale" e modifica alcuni atti legislativi dell'Unione Europea.

[131] «Carta dei diritti fondamentali dell'Unione Europea» (2009) art. 21 Non discriminazione: 1. È vietata qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, la disabilità, l'età o l'orientamento sessuale. 2. Nell'ambito d'applicazione dei trattati e fatte salve disposizioni specifiche in essi contenute, è vietata qualsiasi discriminazione in base alla nazionalità.

[132] «Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza

Andrea Jelinek, presidente dell'EDPB, e Wojciech Wiewiórowski, EDPS, hanno sancito come "Deploying remote biometric identification in publicly accessible spaces means the end of anonymity in those places. Applications such as live facial recognition interfere with fundamental rights and freedoms to such an extent that they may call into question the essence of these rights and freedoms. [...] A general ban on the use of facial recognition in publicly accessible areas is the necessary starting point if we want to preserve our freedoms and create a human-centric legal framework for AI".[133]

3.2 Risoluzione del Parlamento Europeo per il divieto dell'uso TRF

Come si può notare dalla trattazione fin qui svolta, si avverte forte preoccupazione da parte delle istituzioni per l'impiego delle TRF negli spazi pubblici, nonostante le diverse disposizioni normative che ad ora sono state emanate circoscrivano il loro impiego a determinati contesti considerati critici. A condividere la posizione assunta dai due organismi per la protezione dei dati, l'EDPS e l'EDPB, si colloca il Parlamento europeo, il quale il 6 ottobre 2021, ha votato a maggioranza una risoluzione per chiedere alla Commissione europea di vietare, con atto normativo generale, l'utilizzo di sistemi di riconoscimento facciale da parte dell'Unione, in modo che tale tecnologia possa venir usata solo per il riconoscimento di individui già sospetti di aver compiuto crimini e non per controllare dunque in modo generalizzato le persone negli spazi pubblici.

In tale risoluzione si richiede una regolamentazione che vieti l'uso di banche dati private che utilizzino la tecnologia di intelligenza artificiale per schedare volti, quali ad esempio Clearview AI.[134] Sulla scia di tale proposta si è posta la Francia, dove la *Commission nationale de l'informatique et des libertés* (CNIL) il 16 dicembre 2021 ha

artificiale)» (European Data Protection Supervisor, 18 giugno 2021); Foo Yun Chee, «EU Privacy Watchdogs Call for Ban on Facial Recognition in Public Spaces», *Reuters*, 21 giugno 2021, par. Technology, https://www.reuters.com/technology/eu-privacy-watchdogs-call-ban-facial-recognition-public-spaces-2021-06-21/.

[133] «EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination | European Data Protection Supervisor», 21 giugno 2021, https://edps.europa.eu/node/7131_de.

[134] «Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale ne diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI))» (Parlamento europeo, 6 ottobre 2021).

ordinato alla società Clearview AI di cessare il trattamento illegale e di cancellare tutte le foto entro due mesi. L'autorità ha aperto un'indagine a maggio 2020, a seguito di alcuni reclami, avvalorati un anno dopo dalla denuncia mossa dall'associazione *Privacy International*, in merito all'abuso dei dati raccolti dal programma. Specificamente il CNIL evidenzia la violazione del GDPR sotto il profilo della liceità del trattamento dei dati, in quanto sarebbe avvenuto privo di fondamento giuridico, così come previsto dall'art. 6 paragrafo 1 GDPR; e sotto il profilo della mancata presa in considerazione dei dati delle persone fisiche, in rifermento alle richieste di accesso ai propri dati, violando gli artt. 12, 15, 15 del GDPR.[135]

L'adozione di tale risoluzione ha suscitato fin da subito il dibattito all'interno del Parlamento Europeo, vedendo schierati in modo opposto i partiti: a sostegno del divieto si sono posti i gruppi liberali, socialdemocratici, di sinistra e verdi, mentre in netta opposizione si sono collocati i deputati del Partito Popolare Europeo. Tra questi ultimi Alex Voss ha sostenuto come un totale divieto ignora i vantaggi che da questa tecnologia si può trarre.[136]

Nel documento si possono evidenziare alcuni punti che vengono posti all'attenzione della Commissione per una futura regolazione. In primis il Parlamento richiede di porre attenzione ai problemi legati alle discriminazioni che appaiono centrali nell'impiego di TRF, come emerge chiaramente dallo studio elaborato dalle ricercatrici Buolamwini e Gebru. Ma non solo, come sono già emersi fino ad ora esistono altri problemi legati all'impiego delle TRF: la sorveglianza di massa, la trasparenza nell'uso degli strumenti in questione, la polizia predittiva, la valutazione d'impatto.[137]

La risoluzione del Parlamento europeo segue la linea già assunta dall'Alto Commissario ONU per i diritti umani e dal Garante europeo, i quali si sono già

[135] «Facial recognition: the CNIL orders CLEARVIEW AI to stop reusing photographs available on the Internet | CNIL», consultato 7 febbraio 2022, https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet; Regolamento UE 2016/679, GDPR, General Data Protection Regulation artt. 6, 12, 15,17.

[136] Luca Bertuzzi, «Facial recognition technologies already used in 11 EU countries and counting, report says», 26 ottobre 2021, par. Data protection, https://www.euractiv.com/section/data-protection/news/facial-recognition-technologies-already-used-in-11-eu-countries-and-counting-report-says/.

[137] «Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale ne diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI))».

espressi evidenziando come l'impiego di sistemi di AI sia pericoloso per la salvaguardia dei diritti umani e dei valori europei.[138]

Sebbene l'esigenza di una regolamentazione di tali tecnologie appaia necessaria, anche in tempi piuttosto ristretti, il progetto di legge presentato ad aprile 2021 dalla Commissione Europea si trova ancora al vaglio delle istituzioni, in attesa di essere approvato o modificato. Bisognerà attendere dunque l'emanazione di tale nuovo regolamento, per comprendere l'orientamento che le autorità europee adotteranno nella regolazione del settore della AI, anche se, dall'analisi fin qui condotta e alla luce del progetto ideato dalla Presidente della Commissione "un'Unione più ambiziosa", sembra propenso verso una regolamentazione, piuttosto che per un divieto assoluto. Se tale potrà dirsi la direzione che le istituzioni assumeranno, appare come la tecnologia, se usata con rigore, e trasparenza, può offrire notevoli benefici nella vita di ciascuno di noi.

3.3 Attuali utilizzi delle TRF da parte di sistemi informatici dell'UE

Attualmente le TRF sono sfruttate da molteplici autorità al fine di salvaguardare la sicurezza pubblica: si riscontra infatti un ampio utilizzo della tecnologia nel settore dell'immigrazione. I sistemi informatici che sfruttano tali tecnologie sono stati creati al fine di promuovere lo scambio di dati e informazioni: sono strutturati in database gestiti a livello centralizzato e in *network* che pongono in collegamento istituzioni e organismi dell'UE con gli Stati membri. L'unico sistema informatico che non utilizza le TRF è l'ETIAS, il sistema europeo di informazione e autorizzazione viaggi.[139]

L'impiego di tali strumenti è reso possibile dal fatto che il soggetto ha piena consapevolezza dell'utilizzo di TRF da parte delle autorità, perciò, ne consegue che l'identificazione non si svolge nell'ignoranza dell'individuo.

L'utilizzo delle immagini personali, come degli altri dati biometrici, è regolato da leggi, che sanciscono il rispetto del principio di necessità operativa per l'accesso a tali

[138] «The Right to Privacy in the Digital Age», Report of the United Nations High Commissioner for Human Rights (High Commisioner forHuman Rights, 13 settembre 2021); «Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale)», 5.

[139] «Comunicazione della Commissione al Parlamento europeo e al Consiglio. Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia COM (2010)385» (Commissione europea, 20 luglio 2010).

sistemi informatici e prevedono diritti degli interessati in linea con il GDPR. Inoltre, il sistema eu-LISA, l'agenzia europea per la gestione operativa dei sistemi IT su larga scala, è responsabile della garanzia della qualità e si occupa dei meccanismi automatizzati di controllo della qualità dei dati.

Tali strumenti, concepiti per scopi diversi, a seguito di alcune modifiche, stanno sempre più convergendo verso obbiettivi comuni. Dunque, il risultato ottenuto corrisponde ad una confusione tra il settore di gestione dell'immigrazione e quello di contrasto al crimine e al terrorismo: si potrebbe a tal fine parlare di "*crimmigration*", termine coniato da Juliet Stumpf, per indicare una sovrapposizione tra le leggi sull'immigrazione e quelle sulla criminalità.[140]

In generale i sistemi informatici che impiegano la tecnologia di riconoscimento facciale sono: il sistema d'informazione Schengen (SIS), l'European dactylographic (EURODAC), il sistema di informazione visti (VIS), sistema di ingressi/uscite (Entri/exit System – EES), il sistema europeo di informazione sui casellari giudiziari (*European Criminal Records Information System* – ECRIS).

3.3.1 Il sistema d'informazione Schengen (SIS)

Il primo sistema ad impiegare la tecnologia di riconoscimento facciale è il sistema d'informazione Schengen (SIS), che nasce in concomitanza con l'adozione della Convenzione Schengen: l'obbiettivo perseguito è la realizzazione di un sistema in cui vengano meno le frontiere all'interno dell'UE, rafforzando i controlli alle frontiere esterne e la sicurezza pubblica al suo interno. La normativa di tale materia la si rinviene all'art. 3 del TUE e nel titolo V del TFUE. Il fondamento normativo del SIS si colloca, a seguito della nascita del Trattato di Lisbona, all'art. 3 TUE[141] e nel titolo V del TFUE.

[140] Juliet Stumpf, «The crimmigration crisis: immigrants, crime, and sovereign power», *American University Lae Review* 56, n. 2 (2016): 367 ss., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=935547; Mobilio, *Tecnologie di riconoscimento facciale p. 247-250*; «Facial recognition technology: fundamental rights considerations in the context of law enforcement».

[141] «Art. 3 Trattato sull'Unione Europea» 1. L'Unione si prefigge di promuovere la pace, i suoi valori e il benessere dei suoi popoli. 2. L'Unione offre ai suoi cittadini uno spazio di libertà, sicurezza e giustizia senza frontiere interne, in cui sia assicurata la libera circolazione delle persone insieme a misure appropriate per quanto concerne i controlli alle frontiere esterne, l'asilo, l'immigrazione, la prevenzione della criminalità e la lotta contro quest'ultima. 3. L'Unione instaura un mercato interno. Si adopera per lo sviluppo sostenibile dell'Europa, basato su una crescita

A seguito degli attentati terroristici che hanno coinvolto gli Stati Uniti prima, e successivamente nel 2004 Madrid e nel 2005 Londra, il sistema d'informazione Schengen è sempre più stato utilizzato nell'indagine volta a garantire la sicurezza interna.

Il SIS ha subito un'evoluzione nel 2006, a seguito del Regolamento europeo 1987/2006 e della decisione 2007/533/GAI (Giustizia e affari interni), che ha generato il SIS II: si è cercato di dare maggiore attenzione alla sicurezza interna, ampliando i poteri della autorità in questo ambito e la tipologia di dati conservati nei database del sistema. Non più semplicemente dati alfanumerici, ma anche biometrici, quali foto e impronte. Il SIS, dunque, ha acquisito anche la funzione di investigazione ad ampio spettro sulla popolazione.

Il SIS ha subito un'ulteriore modifica a seguito degli attentati che hanno colpito la Francia nel 2015 e il Belgio nel 2016. Nel 2018 sono stati emanati tre regolamenti europei che vanno a regolare tre settori diversi:

- Il regolamento 2018/1862, nell'ambito della cooperazione di polizia e della cooperazione giudiziaria in materia penale, ha l'obbiettivo di garantire la salvaguardia della sicurezza dell'Unione Europea e degli stati membri che hanno aderito al patto Schengen, mediante l'inserimento e l'elaborazione di avvisi di arresto, di persone scomparse e di controlli. Per il perseguimento di tale fine è previsto l'uso di dati biometrici, incluse le immagini del volto di una persona, da parte delle autorità: la disciplina dell'inserimento, della verifica e della ricerca è presente agli artt. 42 e 43 del presente regolamento. Il considerando 22 prevede che "L'uso di immagini del volto e di fotografie a fini

economica equilibrata e sulla stabilità dei prezzi, su un'economia sociale di mercato fortemente competitiva, che mira alla piena occupazione e al progresso sociale, e su un elevato livello di tutela e di miglioramento della qualità dell'ambiente. Essa promuove il progresso scientifico e tecnologico. L'Unione combatte l'esclusione sociale e le discriminazioni e promuove la giustizia e la protezione sociali, la parità tra donne e uomini, la solidarietà tra le generazioni e la tutela dei diritti del minore. Essa promuove la coesione economica, sociale e territoriale, e la solidarietà tra gli Stati membri. Essa rispetta la ricchezza della sua diversità culturale e linguistica e vigila sulla salvaguardia e sullo sviluppo del patrimonio culturale europeo. 4. L'Unione istituisce un'unione economica e monetaria la cui moneta è l'euro.5. Nelle relazioni con il resto del mondo l'Unione afferma e promuove i suoi valori e interessi, contribuendo alla protezione dei suoi cittadini. Contribuisce alla pace, alla sicurezza, allo sviluppo sostenibile della Terra, alla solidarietà e al rispetto reciproco tra i popoli, al commercio libero ed equo, all'eliminazione della povertà e alla tutela dei diritti umani, in particolare dei diritti del minore, e alla rigorosa osservanza e allo sviluppo del diritto internazionale, in particolare al rispetto dei principi della Carta delle Nazioni Unite6. L'Unione persegue i suoi obiettivi con i mezzi appropriati, in ragione delle competenze che le sono attribuite nei trattati.

di identificazione dovrebbe inizialmente aver luogo solo presso i valichi di frontiera regolari. Tale uso dovrebbe essere oggetto di una relazione della Commissione che confermi che la tecnologia necessaria è disponibile, pronta ad essere usata e affidabile."

Tale normativa abroga il precedente regolamento 1986/2006.[142]

- Il regolamento 2018/1861 disciplina l'ambito dei controlli alle frontiere. Lo scopo è quello di inserire ed elaborare segnalazioni al fine di rifiutare l'ingresso o il soggiorno in stati membri dell'area Schengen. Anche in tal caso è ammesso l'uso di dati biometrici, incluse le immagini del volto: la disciplina è presente agli artt. 32 e 33 del presente regolamento. Al considerando 22 si prevede che le immagini del volto e le fotografie dovrebbero essere utilizzate inizialmente, ai fini di identificazione, solo nel contesto dei valichi di frontiere regolari. Tale regolamento abroga quello precedente, il reg. 1987/2006.[143]
- Il regolamento 2018/1860 dispone una normativa nel caso del rimpatrio di cittadini di paesi terzi il cui soggetto è irregolare. L'art. 4 sancisce che l'immagine del volto delle persone deve essere inserita al ritorno solo per confermare l'identità della persona. Questo regolamento per quanto non disciplinato fa riferimento espresso al regolamento 2018/1861.[144]

I tre regolamenti precedentemente non in vigore, lo sono diventati a partire dal 28 dicembre 2021 e in questo modo sono andati a sostituire il SIS II.

Ciascuna normativa del SIS presenta delle disposizioni che hanno un contenuto simile in merito alla protezione delle informazioni del soggetto: le segnalazioni nel SIS devono rispettare il principio di proporzionalità, la sicurezza, la protezione e la conservazione dei dati personali.[145]

I regolamenti, accogliendo l'opinione dello European Data Protection Supervisor, prevedono che l'utilizzo delle immagini, allo scopo di interrogare il SIS può avere

[142] «Regolamento (UE) 2018/1862».

[143] «Regolamento (UE) 2018/1861».

[144] «Regolamento (UE) 2018/1860»; Regolamento (UE) 2018/1861.

[145] Artt. 10,12,21,53,54,66-71«Regolamento (UE) 2018/1862»; Artt. 19, 51-57 «Regolamento (UE) 2018/1861»; «Regolamento (UE) 2018/1860» .

luogo solo per la conferma dell'identità, e non come elemento di identificazione.[146] È previsto inoltre che l'inserimento e l'utilizzo dei volti deve essere limitato a quanto necessario ai fini degli obbiettivi perseguiti, dovrebbe essere autorizzato dal diritto dell'UE e avvenire nel rispetto dei diritti fondamentali, in particolar modo del minore.

La normativa prevede che l'uso di TRF potrà diventare lo strumento principale per realizzare direttamente l'identificazione preposta alle molteplici finalità di decisione, controllo e contrasto.

Il Garante europeo per la privacy ha espresso grande preoccupazione in relazione alla disciplina contenuta in tali regolamenti, in termini di qualità di dati impiegati, necessità e proporzionalità nell'utilizzo degli indicatori biometrici per gli scopi indicati, rispetto delle previsioni generali del GDPR e dalla LED. L'EDPS ha dunque sollecitato affinché si realizzi un più chiaro e diretto collegamento con tali disposizioni generali, riferite alla limitazione della finalità, utilizzo di sistemi di sicurezza all'avanguardia, periodi di tempo proporzionati per la conservazione dei dati, qualità e protezione degli stessi fin dalla progettazione, tracciabilità, supervisione efficace e sanzioni dissuasive per usi impropri.[147] Ciò al fine di rispettare gli standard di qualità dei dati stabiliti dallo stesso: la necessità di usare identificatori biometrici deve essere chiaramente dimostrata e la possibilità di beneficiarne devono dipendere da misure di salvaguardia più stringenti.[148]

3.3.2 Il sistema Europan dactylographic (EURODAC)

Il secondo sistema informatico è l'European dactylographic (EURODAC): è il database europeo delle impronte digitali, per coloro che richiedono asilo e per le persone fermate nel varcare una frontiera esterna in modo irregolare. Viene istituito con il regolamento 2725/2000/CE[149], al fine di agevolare l'applicazione della

[146] «Opinion 7/2017 on the new legal basis of the Schengen Information System» (European Data Protection Supervisor, 2 maggio 2017) n. 19; art. 43 Regolamento (UE) 2018/1862; art. 33 Regolamento (UE) 2018/1861.

147 «Facial recognition technology: fundamental rights considerations in the context of law enforcement»; Mobilio, Tecnologie di riconoscimento facciale p. 251-256.

[148] «EDPS Formal comments on the draft Commission Implementing Decisions» (European Data Protection Supervisor, 26 agosto 2020).

[149] «Regolamento 2725/2000/CE» (2000).

Convenzione di Dublino, stipulata per la determinazione dello stato responsabile per l'esame di domande di protezione internazionale proposte da cittadini di paesi terzi o da apolidi. L'obbiettivo è verificare le impronte digitali di coloro che entrano illegalmente nell'area Schengen, al fine constatare che non si realizzi il fenomeno di *asylum shopping* in cui vengono formulate più domande in diversi stati.

Gli scopi di tale sistema informatico sono stati ampliati a seguito delle modifiche introdotte dal regolamento 603/2013[150], che ha introdotto una disciplina più precisa dei diritti dei soggetti a cui questa si riferisce e delle politiche di pubblica sicurezza, per un maggiore controllo dell'immigrazione irregolare e dei movimenti secondari. L'uso del sistema EURODAC ha carattere residuale rispetto all'utilizzo delle altre banche dati: può essere usato solo se il confronto non ha consentito di stabilire l'identità dell'interessato. È stabilito inoltre che può essere sfruttato nel caso in cui il confronto sia necessario: ai fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi; in un caso specifico; o contribuisca in misura sostanziale alla prevenzione, all'individuazione o all'investigazione di uno dei reati in questione.[151]

Nel 2016 la Commissione ha presentato un progetto di modifica dell'EURODAC, che prevede l'uso di immagini del volto da archiviare e trasmettere alle autorità di polizia, per il controllo dell'immigrazione clandestina, dei movimenti secondari dei cittadini di paesi terzi all'interno dell'UE e dell'identificazione degli immigrati irregolari.[152]

Tale proposta di modifica però non è stata accolta, a seguito dell'opposizione dei paesi quali Polonia, Ungheria, Repubblica Ceca e Slovacchia. In merito si è espresso anche il Garante europeo della protezione dati, che ha espresso la sua preoccupazione in relazione alla presenza di "alcuna valutazione sulla necessità di raccogliere e utilizzare le immagini del volto delle categorie di persone interessate dalla proposta di rifusione Eurodac. Inoltre, l'EDPS ritiene che la proposta debba chiarire i casi in cui espletare un confronto delle impronte digitali e/o delle immagini del volto, dal

[150] «Regolamento (UE) 603/2013» (2013).

[151] Art. 20 Regolamento (UE) 603/2013.

[152] «Proposta riforma regolamento (UE) 2016/0132» (2016).

momento che la stesura della proposta di rifusione sembra implicare un confronto sistematico".[153]

3.3.3 Il sistema di informazione visti (VIS)

Il sistema di informazione visti (VIS) è uno strumento di scambio di dati e informazioni relativi ai visti d'ingresso nello Spazio Schengen rilasciati ai cittadini di paesi terzi; è posto inoltre a controllo delle frontiere nell'area Schengen.

Il sistema nasce all'indomani degli attentati dell'11 settembre 2001, dunque con scopi principalmente antiterroristici.

La disciplina del VIS è presente nel regolamento (CE) 767/2008[154], per le materie relative al "primo pilastro", e nella decisione 2008/633/GAI[155], per quanto attiene al "terzo pilastro": l'obbiettivo è la costruzione di una disciplina comune in materia di visti e il rafforzamento di una politica di sicurezza pubblica, che vada ad intensificare i controlli alla frontiera e, all'interno degli stati membri, rendere più facile l'identificazione degli immigrati irregolari. A tal fine il sistema può sfruttare i dati alfanumerici, quali le generalità, provenienza, scopo del viaggio, fotografie e impronte digitali. Le immagini del volto possono essere usate solo nel caso in cui l'uso degli altri dati non consenta di raggiungere gli scopi perseguiti. Inoltre, è consentito l'utilizzo solo nel caso in cui si tratti della materia di immigrazione e asilo.

Nel caso in cui il VIS venga sfruttato per scopi di pubblica sicurezza sono previste delle restrizioni, volte a garantire il principio di necessità e proporzionalità nell'uso dei dati. Sono inoltre disposte garanzie volte a tutelare il trattamento dei dati: l'art. 37[156] prevede che l'individuo debba essere informato sullo scopo del trattamento.

---

[153] Giuseppe Morgese, «La riforma del sistema Dublino: il problema della condivisione delle responsabilità», *Diritto pubblico*, n. 1 (aprile 2020): 103 ss., https://doi.org/: 10.1438/96677; «Sintesi del parere del Garante europeo della protezione dei dati relativo al primo pacchetto di riforme sul sistema europeo comune di asilo (regolamenti Eurodac, EASO e Dublino) 2017/C 9/04 n.72» (Garante europeo della protezione dati, 2017); Mobilio, *Tecnologie di riconoscimento facciale*, 257–60; «Facial recognition technology: fundamental rights considerations in the context of law enforcement».

[154] «Regolamento (CE) 767/2008» (2008).

[155] «Decisione 2008/633/GAI» (2008).

[156] Art. 37 Regolamento (CE) 767/2008.

Nel 2018, a seguito degli attentati terroristici di Madrid del 2015 e di Londra del 2016, la Commissione ha proposto una riforma volta a permettere al VIS di sfruttare i sistemi di riconoscimento facciale: in questo modo le immagini rilevate dal vivo possono essere utilizzate in sistemi automatizzati a scopi di confronto e non identificazione.[157]

3.3.4 Il sistema ingressi/uscite (EES)

Il sistema di ingressi/uscite (Entri/exit System – EES) si inserisce nel pacchetto "frontiere intelligenti", elaborato dalla Commissione europea nel 2013, volto a rendere più affidabili le procedure di controllo alle frontiere, mediante l'applicazione delle tecnologie avanzate interconnesse nell'insieme dello spazio Schengen.[158]

La disciplina del EES è contenuta nel regolamento (UE) 2017/2226. Il sistema è stato concepito per il controllo dei soggiorni di breve durata o che sono esenti dal visto, al fine di garantire un'identificazione sistematica, e per la sicurezza pubblica contro il pericoli di attacchi terroristici o altri gravi crimini.[159]

Il sistema è complementare al VIS, perché è rivolto per la durata della permanenza dei cittadini di paesi terzi che richiedono il visto, e all'EURODAC, dal quale si differenzia per il diverso titolo di ingresso e la legittimità della permanenza dei cittadini. Si tratta infatti di uno strumento rivolto ai viaggiatori provenienti da paesi terzi, che entrano legalmente sul territorio. Il sistema registra il nome della persona, il tipo di documento di viaggio, i dati biometrici, quali impronte digitali e immagini del volto, e la data e il luogo di entrata e di uscita, sempre nel rispetto dei diritti fondamentali e della protezione dati: viene creato così un fascicolo individuale per ciascun transitante. Vengono dunque sfruttate tecnologie di riconoscimento facciale: l'immagine rilevata sul posto oppure estratta dal documento di viaggio

[157] Mobilio, *Tecnologie di riconoscimento facciale p.260-264*; «Facial recognition technology: fundamental rights considerations in the context of law enforcement»; «Regolamento (CE) 767/2008» (2008).

[158] «Frontiere intelligenti» (Parlamento europeo, 4 giugno 2015).

[159] «Explanatory Memorandum COM (2016) 194 final 2016/0106 (COD)» (Commissione europea, 6 aprile 2016).

elettronico deve godere di una buona risoluzione e qualità per poter essere confrontata.[160]

L'EES sostituisce il metodo tradizionale di timbratura manuale dei passaporti, che rendeva il processo molti più lento e meno efficiente.[161]

Possono accedere al sistema solo le autorità autorizzate dagli stati e competenti circa i controlli di frontiera, i visti e l'immigrazione, per il compimento di attività istituzionalizzate o a scopi identificativi.[162]

L'EES unito all'ETIAS, il sistema europeo di informazione e autorizzazione dati, costituiscono un sistema complessivo di sorveglianza biometrica rivolta a tutti i viaggiatori che si muovono in modo legale nell'area Schengen da paesi terzi. Ciò realizza un sistema di raccolta massiva e intrusiva di dati e informazioni personali, che rischia di violare l'art. 52 della Carta dei diritti fondamentali dell'UE[163], il quale prevede il rispetto del principio di necessità e proporzionalità nel trattamento dei dati. Uno dei rischi più pericolosi di tale struttura si verifica nel caso in cui tale sistema non venga utilizzato per indagare soggetti sospettati di aver tenuto condotte criminose, ma come mezzo per il controllo di soggetti non sospetti. La Corte di Giustizia si è espressa in merito sottolineando come sia necessario che tali mezzi vengano impiegati solo laddove emerga un chiaro nesso tra il comportamento sorvegliato e il realizzarsi di una fattispecie criminosa. A ciò si aggiunge anche la preoccupazione espressa dal Garante europeo per la protezione dei dati, che considera inaccettabile che l'ESS possa essere direttamente e principalmente sfruttato per finalità di polizia e non esclusivamente per questioni di controlli alle frontiere.[164]

---

[160] «Regolamento (UE) 2017/2226» (2017).

[161]«Entry-Exit System», European Commission, s.d., https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en.

[162] «Facial recognition technology: fundamental rights considerations in the context of law enforcement»; Mobilio, *Tecnologie di riconoscimento facciale p. 265-269*.

[163] Carta dei diritti fondamentali dell'Unione Europea art. 52 co.1: Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

[164] C-203/15 e C-698/15, Tele2 Sverige AB (CGUE 21 dicembre 2016) p. 105; «Opinion 06/2016 on the second EU SmartBorders Package Recommendations on the revised Proposal to establish an Entry/Exit System n. 19» (European Data Protection Supervisor, 21 settembre 2016).

3.3.5 Il sistema informatico del casellario giudiziale europeo ECRIS-TNC

Il sistema europeo di informazione sui casellari giudiziari (*European Criminal Records Information System* - ECRIS) è stato istituito nell'aprile 2012 per migliorare lo scambio di informazioni sui casellari giudiziari in tutta l'UE. Tale strumento permette infatti lo scambio uniforme e rapido di informazioni sulle condanne tra i paesi dell'UE, fornisce ai giudici un facile accesso alle informazioni sui precedenti delle persone interessate ed elimina la possibilità che un soggetto condannato in un paese UE possa sottrarsi alle conseguenze delle proprie trasgressioni in un altro paese membro.

Nel 2017 la Commissione ha presentato una proposta volta ad istituire il sistema ECRIS-TNC centralizzato, gestito da eu-LISA, al fine di integrare la mancanza di informazioni su cittadini extra-UE. Nella primavera del 2019 è stato raggiunto l'accordo sul regolamento di questo strumento, che dovrebbe entrare in vigore nel 2022.

Il regolamento 2019/816[165], che disciplina tale sistema, prevede che per ciascun soggetto sia creato un fascicolo contenente i dati alfanumerici, le impronte digitali e le immagini del volto. Quest'ultime possono essere usate in un primo momento, a scopo di conferma di interrogazioni di dati alfanumerici; non possono essere usate direttamente a scopo identificativo.[166]

3.3.6 Interoperabilità

La Commissione europea, nella comunicazione "Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza" dell'aprile 2016[167], ha evidenziato la necessità di una riforma dell'architettura dei sistemi informatici volta a migliorare la gestione dei dati in UE per il controllo delle frontiere e della sicurezza, ma anche per risolvere la crescente frammentazione dovuta alla presenza di una pluralità di

[165] «Regolamento (UE) 2019/816» (2019).

[166] Artt. 5-6 Regolamento (UE) 2019/816; Mobilio, *Tecnologie di riconoscimento facciale*, 271; «European Criminal Records Information System (ECRIS)», European Commission, s.d., https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/tools-judicial-cooperation/european-criminal-records-information-system-ecris_en.

[167] «Comunicazione della Commissione Europea al Parlamento europeo e al Consiglio, Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza», 2016.

strumenti diversi che trattano gli stessi dati. L'obbiettivo è realizzare l'interoperabilità tra i sistemi: si tratta della capacità di comunicare, di scambiare dati e farne utilizzo, al fine di ottenere dei risultati ottimali che assicurino il rispetto dei diritti fondamentali.[168]

Il fondamento legislativo si rinviene in due regolamenti, il regolamento 2019/817[169] in materia di frontiere e visti, e il regolamento 2019/818[170] per quanto attiene alla cooperazione giudiziaria e di polizia, asilo e migrazione, entrambi del maggio 2019.

Questo sistema permette agli stati UE di poter accedere a tutti i dati, comprese le immagini del volto, riguardanti cittadini dell'Unione Europea e di stati terzi, presenti nei sistemi dell'UE: SIS, VIS, EURODAC, EES, ECRIS-TNC e ETIAS.

I due regolamenti perseguono una pluralità di fini, quali il miglioramento del controllo delle frontiere esterne, la politica comune in materia di visti, l'esame delle domande di protezione internazionale, l'identificazione di persone ignote, la prevenzione e la lotta all'immigrazione illegale, il mantenimento della sicurezza pubblica e l'ordine pubblico, la prevenzione e la lotta ai reati di terrorismo o altri reati gravi.[171]

La nuova architettura vede l'aggiunta di altri quattro strumenti: *l'European Search Portal* (ESP), *shared biometric matching service* (BMS), il *common identity repository* (CIR) e il *multiple-identity detector* (MID).

L'ESP è uno strumento volto a fungere da interfaccia unica in grado di consentire l'interrogazione parallela di tutti i citati sistemi di informazione dell'UE, dei dati Europol e delle banche dati Interpol, da parte di stati membri e delle agenzie dell'UE.

Il BMS è un sistema in grado di raccogliere tutti i *template* biometrici, comprese le immagini dei volti, presenti nei diversi sistemi. È possibile dunque realizzare un confronto traversale su tutti i template presenti nei diversi sistemi IT, senza dover compiere indagini separate.

---

[168] «Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice» (European Data Protection Supervisor, 17 novembre 2017) p.7.

[169] «Regolamento (UE) 2019/817» (2019).

[170] «Regolamento (UE) 2019/818» (2019).

[171] Art. 2 par. 1 «Regolamento (UE) 2019/817» (2019); Art. 2 par. 1«Regolamento (UE) 2019/818» (2019).

Il CIR invece è un database entro cui confluiscono i dati personali provenienti da VIS, EURODAC, EES, ETIAS e ECRIS-TNC, nel quale vengono creati fascicoli individuali contenenti dati personali, compresi quelli biometrici.

Il MID è un sistema in grado di creare un fascicolo individuale su ogni soggetto, stabilendo collegamenti tra i dati dei sistemi di informazione dell'UE inclusi nel CIR e i dati del SIS, e che consente il rilevamento delle identità multiple, al duplice scopo di agevolare le verifiche di identità e contrastare la frode di identità.[172]

Questo sistema di interoperabilità ha suscitato però dubbi in merito al quadro giuridico già complesso in cui operano tali sistemi. In tal senso si è espressa la Corte di Giustizia che ha condannato tale architettura volta a creare una sorta di sorveglianza costante e generalizzata, che viola il diritto alla vita privata e alla protezione dei dati personali così come protetti dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'UE.[173] Inoltre, la Corte si è espressa nella sentenza *Tele2 Sverige*, stabilendo come siano strettamente necessari dei criteri oggettivi per definire le modalità e le condizioni da rispettare per l'accesso a tali dati, onde evitare il realizzarsi di un controllo costante della società.[174]

Questa architettura che sfrutta ampiamente le immagini delle persone potrebbe produrre forti discriminazioni in relazione all'uso di TRF, visti i margini d'errore relativi alla qualità dei dati o alle caratteristiche dei soggetti coinvolti, con il rischio di creare falsi-positivi o falsi-negativi. A tutela di ciò l'art. 5[175] contiene una clausola di non discriminazione, volta a tutelare i diritti fondamentali. Inoltre, risulta necessario garantire la qualità dei dati e delle immagini: eu-LISA deve prevedere meccanismi automatizzati di controllo.

[172] Art. 25 Regolamento (UE) 2019/817; Art. 25 Regolamento (UE) 2019/818.

[173] C-293/12 e C-594/12 Digital Rights Irleand (CGUE 8 aprile 2014); Carta dei diritti fondamentali dell'Unione Europea Art 7: Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni. Art. 8 1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

.

[174] C-203/15 e C-698/15, Tele2 Sverige AB.

[175] Regolamento (UE) 2019/817; Regolamento (UE) 2019/818.

Secondo quanto sostiene l'European Data Protection Supervisor il sistema così ideato realizza un punto di non ritorno nell'interpretazione giuridica di alcuni principi e nel modo in cui i dati personali verranno trattati dagli stati e dall'UE.[176]

Il rischio in cui si incorre dunque è la realizzazione di una sorveglianza di massa che, oltre ad osservare i cittadini, va a creare una conoscenza approfondita di identità, abitudini e comportamenti.[177]

3.4 Primo caso di utilizzo di TRF in UE portato di fronte ad una Corte: Cardiff

Il primo caso di utilizzo di TRF dal vivo da parte degli organi di polizia in Europa, che è stato portato di fronte ad una Corte, si rinviene nel Regno Unito a Cardiff, nella finale di UEFA Champions League del 2017.

La polizia del Galles ha attuato il progetto-pilota "*Automated Facial Recognition (AFR) Located*", con il quale vengono impiegate videocamere di sorveglianza, ad uso *live*, al fine di riprendere immagini digitali di persone tra la folla e procedere alla loro identificazione in tempo reale. Le immagini vengono processate e comparate con quelle presenti in appositi database, *watchlist*, confezionati per usi specifici: trattasi generalmente di soggetti posti all'attenzione della polizia in quanto ricercati, aventi precedenti o la cui presenza può essere pericolosa in determinate occasioni. Tale sistema sfrutta la TRF e tramite le immagini presenti nella *watchlist* e quelle catturate dal vivo, propone un'identificazione che deve essere confermata dall'operatore umano: in caso di riscontro negativo viene eliminata la foto, nel caso di esito positivo l'immagine viene salvata per 24 ore e sarà necessario l'intervento dell'agente per fermare il soggetto in questione.

Tuttavia, la polizia del Galles meridionale non si è limitata ad usare tali strumenti solo in occasione di eventi specifici: l'utilizzo delle TRF è stato impiegato nelle ordinarie azioni di prevenzione, indagine e repressione di reati, tanto che si conta che siano state utilizzate tra il 2017 e il 2019 in 50 occasioni diverse. Le forze di polizia hanno tuttavia informato i cittadini dell'impiego di tali strumenti, dandone preventiva

[176] «Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems» (European Data Protection Supervisor, 16 aprile 2018) p. 143.

[177] «Facial recognition technology: fundamental rights considerations in the context of law enforcement»; Mobilio, *Tecnologie di riconoscimento facciale p. 269-285*.

notizia attraverso i social network, distribuendo volantini ed esponendo cartelloni con adeguata informativa nelle aree in cui era in uso.[178]

L'utilizzo delle AFR è giunto all'attenzione dei giudici inglesi che hanno dato prova, nei diversi gradi di giudizio, di come la vicenda possa sollevare interpretazioni contrastanti: la *Court of Appeal* si è espressa in modo opposto rispetto alla *High Court of Justice* sulla vicenda in esame. Il *casus quo* ha origine dalla vicenda di un attivista per i diritti civili, Edward Bridges, che, con il supporto della organizzazione britannica non governativa Liberty, ha adito la *High Court of Justice* censurando di essere stato sottoposto illegalmente al sistema *AFR Locate* in due zone diverse della città di Cardiff, senza il suo consenso e in mancanza di avvisi che informassero che quell'area era sottoposta a tali tecnologie. L'attore non faceva parte dei soggetti inseriti nella *watchlist*, in quanto trattasi di un comune cittadino. Le norme violate, secondo quanto si legge nella decisione della Corte, sarebbero:

1. Il diritto alla privacy e alla vita privata, così come tutelato dall'art. 8 CEDU, tramite lo *Human Rights Act* del 1998;
2. *Data Protection Act* del 2018, adottato in attuazione del GDPR;
3. *Equality Act* del 2018, che ha lo scopo di evitare che vengano ad essere prodotti effetti discriminatori.

Nel settembre 2019 la *High Court* si è espressa in merito al caso in questione con una decisione che respinge la pretesa sollevata dal signor Bridges, sancendo come l'uso della tecnologia di riconoscimento facciale sia contemporaneamente "in accordance with the law" e "necessary and proportionate" per raggiungere gli obblighi di legge previsti. La Corte afferma che i requisiti di proporzionalità e necessarietà sono soddisfatti nel momento in cui la restrizione sia più che semplicemente utile, ragionevole e desiderabile. Inoltre, lo strumento deve essere il meno invasivo tra quelli che hanno la funzione di proteggere e devono essere proporzionati all'interesse che si deve proteggere. I giudici ritengono, contrariamente a quanto sostenuto dall'attivista, che tali requisiti sono soddisfatti. Per le stesse ragioni rigettano le affermazioni secondo cui l'utilizzo di *AFR Locate* violerebbe il *Data Protection Act*. Infine, respingono anche le asserzioni secondo cui la polizia non avrebbe rispettato i suoi obblighi di garantire la non discriminazione e l'equità, come previsto

[178] Andrea Pin, «Non esiste la "pallottola d'argento": l'Artificial Face Recognition al vaglio giudiziario per la prima volta», *DPCE online*, 8 gennaio 2020, http://www.dpce.it/dpce-online.html; Mobilio, *Tecnologie di riconoscimento facciale*, 229–39.

dall'*Equality Act*. Pertanto, la *High Court* conclude affermando "the current legal regime is adequate to ensure the appropriate and nonarbitrary use of AFR Locate, and that *South Wales Police*'s use to date of *AFR Locate* has been consistent with the requirements of the *Human Rights Act*, and the data protection legislation."[179]

A seguito della decisione della *High Court*, espressasi in modo negativo in merito alla pretesa dell'attivista, Bridges nel giugno 2020 ha appellato la sentenza alla *Court of Appeal*, evidenziando 5 punti:

1. La *High Court* avrebbe errato nell'affermare che il diritto alla privacy garantito dall'art. 8 della CEDU non fosse leso dall'utilizzo dell'*AFR Locate*, per via del secondo comma dell'art. 8 CEDU.
2. In secondo luogo, il ricorrente denuncia come la Corte, nel valutare se il requisito della proporzionalità fosse stato rispettato, ha valutato solo l'impatto sulla persona del ricorrente, senza tenere conto dell'impatto complessivo sulle persone che ha avuto l'uso della tecnologia in questione.
3. In terzo luogo, l'appellante lamenta come sia stato erroneamente dichiarato dai giudici, a seguito di una valutazione, la corretta applicazione della normativa da parte delle autorità.
4. Inoltre, Bridges denuncia il mancato esprimersi della Corte sull'assenza di un documento che attesti il rispetto da parte della polizia dei propri doveri.
5. Infine, emerge come la Corte non abbia considerato le discriminazioni indirette che possono emergere dall'uso di *AFR Locate*.

Nell'agosto 2020 la *Court of Appeal* ribalta la sentenza di primo grado della *High Court*, in accordo con tre dei punti denunciati nel ricorso di appello presentato dall'appellante. Secondo quanto si evince dal testo della sentenza la *Court of Appeal* sostiene che l'uso di AFR Locate da parte della polizia non si è svolto in accordo con quanto riportato all'art. 8 co. 2 della CEDU, in quanto il quadro normativo presente lascia troppa discrezionalità al corpo di polizia sulla scelta degli individui da inserire nella *watchlist* e sul luogo dove impiegare le telecamere, risultando dunque non abbastanza prevedibile; inoltre, il Data *Protection Impact Assessment* non sarebbe conforme al *Data Protection Act* del 2018, in quanto non sarebbe stato in grado di calcolare il rischio causato dall'*AFR Locate* per i dritti e le libertà; infine, la Corte

[179] Bridges, R (On Application of) v The Chief Constable of South Wales Police EWHC 2341 (Admin) (Hight Court of Justice 4 settembre 2019).

constata come la polizia gallese non abbia rispettato i doveri stabiliti nella sezione 149 dell'*Equality Act* del 2010, dal momento che ha fallito nel riconoscere che le TRF possono avere un impatto sproporzionato su donne e minoranze.[180]

Il caso del signor Bridges è stato il primo ad affrontare la questione dell'utilizzo ad opera della polizia delle TRF nei luoghi pubblici. Ciò che emerge dalla vicenda va oltre i confini del territorio britannico, in quanto a venire in rilievo è l'importanza di un quadro normativo adeguato, all'interno di ciascun ordinamento, che vada a disciplinare l'utilizzo delle tecnologie di riconoscimento facciale.

Tale decisione evidenzia l'importanza di due elementi, che risultano fondamentali per l'utilizzo dell'AFR Locate: le immagini che non risultano dal *matching* vengono automaticamente cancellate e quelle per cui invece risulta un riscontro necessitano dell'intervento di un agente umano che vada ad approvare il *matching* ottenuto.[181] Nonostante riconosca il diritto dell'attivista, il punto di vista della Corte va a considerare tale riconoscimento in relazione al singolo: l'utilizzo di sistemi di videosorveglianza genera un danno all'individuo, non genera un danno per l'intera società. Infatti, è in virtù di ciò che nel riconoscere tale violazione, non concorda con il ricorrente, che, nel presentare il ricorso d'appello, ha evidenziando come la *High Court of Justice* non abbia considerato come l'uso di TRF vada a violare non solo i suoi diritti, ma quelli della società in generale, con il risultato di ottenere un *chilling effect*. Rimane comunque non chiaro il motivo per cui la Corte non abbia considerato le implicazioni che l'uso di tali strumenti comporta per la collettività. Complessivamente da tale primo caso di utilizzo delle tecnologie di riconoscimento facciale emerge come i giudici inglesi, con tale sentenza, abbiano legittimato l'utilizzo di tali strumenti per la sorveglianza di massa, e contemporaneamente abbiano fallito nel considerare gli effetti a lungo termine che l'uso di tali mezzi può comportare.[182]

[180] R. (On the Application Of) v. South Wales Police [2020] EWCA Civ 1058 (Court of Appeal 11 agosto 2020); Jacopo Della Torre, «Novità del Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice», *Diritto penale contemporaneo - Rivista trimestrale*, 2020.

[181] R. (On the Application Of) v. South Wales Police [2020] EWCA Civ 1058.

[182] Monika Zalnieriute, «Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State», *The Columbia Science & Technology Law Review*, 2021; Hugh Tomlinson, «Case Law: R (on the Application of Bridges) v Chief Constable of South Wales, Police Use of "automatic Facial Recognition Technology Unlawful – Hugh Tomlinson QC», Inforrm's Blog, 17 agosto 2020, https://inforrm.org/2020/08/17/case-law-r-on-the-application-of-bridges-v-chief-constable-of-south-wales-police-use-of-automatic-facial-recognition-technology-unlawful-hugh-tomlinson-qc/.

Una violazione denunciata dal signor Bridges, accolta anche dalla Corte, riguarda le discriminazioni perpetuate dalla *South Wales Police*, dovute al tipo di *training* che i software hanno subito, generalmente effettuato con foto di arresti e condanne, e influenzato dal *background* di disuguaglianze. Donne e minoranze etniche, in particolar modo soggetti appartenenti alla popolazione non caucasica, vedono un numero molto più elevato di falsi positivi: numerose sono le testimonianza e le prove di *bias* che affliggono tali sistemi, come dimostra lo studio realizzato dalle ricercatrici Joy Boulamwini e Timnit Gebru. Sebbene il *training* effettuato dalle società che producono tali software sia segreto, la Corte evidenzia come per salvaguardare l'interesse pubblico ciò che risulta necessario sarebbe l'adozione software *open-source* da parte di forze di polizia e pubbliche autorità.[183]

Sebbene tale sentenza risulti il punto di riferimento per l'imposizione di limiti all'utilizzo di TRF da parte delle forze dell'ordine, rimane comunque troppo debole per avere un impatto a lungo termine sull'uso e sviluppo di tali strumenti: la *Court of Appeal*, al fine di far rispettare il diritto alla privacy e i doveri rientranti nell'*Equality Act*, si è limitata ad imporre limiti formalistici ai poteri della polizia. In questo modo ha aperto alla possibilità che ciascun dipartimento di polizia possa regolare come ritiene corretto l'uso di tali strumenti, comportando dunque una frammentazione della disciplina delle TRF. All'inizio del 2020 il *Metropolitan Police Service* di Londra, ha annunciato che avrebbe impiegato sistemi di riconoscimento facciale come parte della sua strategia di localizzazione.[184]

È auspicabile, dunque, l'emanazione di una legge che vada a creare un quadro normativo più specifico, in modo da poter ridurre la frammentarietà del sistema che si è venuto a creare.

Una delle lacune maggiori in cui incorrono i giudici nel caso di specie, seppur rimanga punto di partenza per la disciplina futura sulla regolazione delle TRF, è l'assenza dell'indicazione del prerequisito della trasparenza nell'uso di tali strumenti: ciò comporta dunque il mantenimento del *favor* per la legge sul segreto commerciale.

[183] Henriette Ruhrmann, «Facing the Future: Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement», maggio 2019; Buolamwini e Gebru, «Gender Shades».

[184] James Vincent, «London Police to Deploy Facial Recognition Cameras across the City», The Verge, 24 gennaio 2020, https://www.theverge.com/2020/1/24/21079919/facial-recognition-london-cctv-camera-deployment.

Ma ancor più grave risulta il fallimento della Corte nel considerare come l'impiego delle tecnologie abbia delle implicazioni su valori fondanti i governi occidentali, quali la democrazia, la pubblica partecipazione e l'identità personale negli spazi pubblici.

In merito all'impiego di tali strumenti ormai diffusi in molti dipartimenti di polizia si è espresso anche l'*Information Commissioner's Office* (ICO), che si è detto molto preoccupato per il potenziale impiego della TRF in modo inappropriato, eccessivo o avventato. Con ciò la *Commissioner* ha espresso come sia necessario l'adozione di norme ad hoc volte a garantire il rispetto dei diritti fondamentali, e non semplici indicazioni formali che lascino liberi gli agenti di polizia nel decidere come meglio impiegare per i propri scopi le tecnologie.[185]

In Gran Bretagna non mancano le opinioni totalmente contrarie all'uso della tecnologia in questione. La sentenza emanata dalla *Court of Appeal* ha generato un grande malcontento in chi sperava che con tale sentenza si potesse giungere ad una totale proibizione delle TRF. A tal fine il 3 febbraio 2020 è stata presentata in Parlamento britannico la richiesta di moratoria, *Automated Facial Recognition Technology (Moratorium and Review) Bill*, volta a proibire l'uso di tali strumenti negli spazi pubblici e a rivedere la disciplina già presente sul suo utilizzo. Tale richiesta è stata firmata non solo da enti volti a tutelare i diritti umani, ma anche da parlamentari e membri della società civile.[186]

In conclusione, a seguito degli esiti giurisprudenziali, alla *South Wales Police* non è stato interdetto l'uso dell'*AFR Locate*. Il suo impiego è ammesso in tutti i casi in cui questo sistema venga impiegato per scopi di indagine, come è avvenuto per l'arresto di un predatore sessuale, reso possibile dallo sfruttamento di TRF che confrontano le immagini riprese con quelle presenti in *watchlist* contenenti foto di soggetti con precedenti condanne.[187]

---

[185] Elizabeth Denham, «Information Commissioner's Opinion Addresses Privacy Concerns on the Use of Live Facial Recognition Technology in Public Places» (ICO, 18 giugno 2021), https://ico.org.uk/about-the-ico/news-and-events/information-commissioner-s-opinion-addresses-privacy-concerns-on-the-use-of-live-facial-recognition-technology-in-public-places/.

[186] «Automated Facial Recognition Technology (Moratorium and Review) Bill [HL] - Parliamentary Bills - UK Parliament», 4 febbraio 2020, https://bills.parliament.uk/bills/2610; Big Brother Watch, «Joint statement on police and private company use of facial recognition surveillance in UK», settembre 2019.

[187] Jenny Rees, «Facial recognition: How South Wales Police caught a sexual predator», *BBC News*, 19 febbraio 2021, par. Wales, https://www.bbc.com/news/uk-wales-55842869.

3.5 L'uso di TRF nei paesi dell'UE

La diffusione di sistemi di sorveglianza remota ha interessato non solo la Gran Bretagna, ma anche molti paesi dell'Unione Europea, nei quali si può constatare come ad un primo impiego di TRF per attività a fini di indagine, si è potuto appurare il crescente interesse da parte delle forze dell'ordine per l'impiego della strumentazione nei più svariati usi nella quotidianità. Emergono dunque programmi pilota attuati per testare l'efficienza dell'impiego di strumenti di riconoscimento facciale in aree prestabilite, che vedono la sottoposizione all'esperimento di soggetti volontari.

Un primo studio, in merito alla diffusione di sistemi di videosorveglianza è stato condotto nel 2019 dalla società da *Surfshark*[188], con l'obbiettivo di individuare quali paesi impieghino costantemente strumenti di riconoscimento facciale in tutto il mondo. Per quanto attiene ai paesi europei, si può constatare come la maggior parte ha adottato o stia adottando tali strumenti.[189]

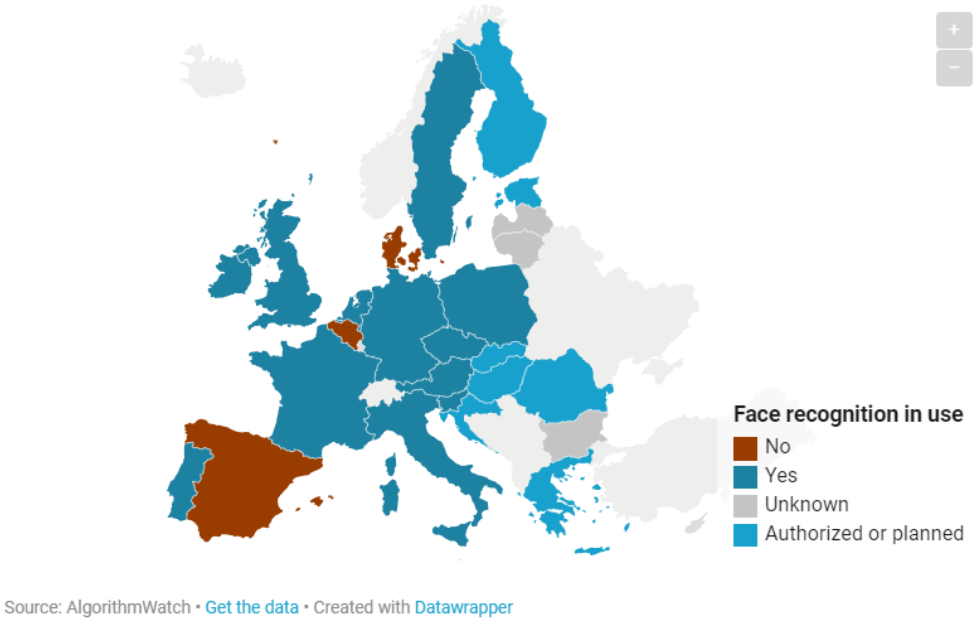
L'organizzazione no-profit di ricerca e advocacy *AlgorithmWatch*, ha effettuato un'ulteriore indagine nel 2019, aggiornata poi nel giugno 2020, sempre con lo scopo di delineare quali stati all'interno dell'Unione Europea impieghino costantemente TRF. Lo studio ha portato alla luce come le forze dell'ordine, generalmente disposte ad utilizzare tali strumenti, con usi che possono variare in ogni paese, condividano una caratteristica comune: l'assenza di trasparenza nel loro impiego. Trasparenza, che si riferisce anche al modo in cui le tecnologie vengono implementate e sviluppate, sia che abbiano natura pubblica che privata. Alla mancanza di tale requisito corrisponde anche la segretezza in merito ai parametri utilizzati, dipesa dal non voler rivelare le informazioni sui dati di *training* del software. Precisamente dallo studio realizzato da *AlgorithmWatch* si evince come, su 25 stati membri dell'UE presi in considerazione:

1. Almeno undici stati utilizzano il riconoscimento facciale;
2. Otto paesi prevedono di introdurre la tecnologia nei prossimi anni;

[188] «Surfshark About Us-products, company, people» Surfshark, https://surfshark.com/it/about-us. Surfshark è una società con sede nei Pesi Bassi che nasce con l'obbiettivo di offrire servizi che permettano alle persone di aver controllo sulle loro vite digitali.

[189] «The Facial Recognition World Map - Smile You're on Camera», Surfshark, 2019, https://surfshark.com/facial-recognition-map.

3. Due, Spagna e Belgio, non lo consentono.[190]



La conferma del quadro appena delineato è offerta inoltre da uno studio commissionato dal gruppo parlamentare *The Greens*, contrario all'uso di tecnologie di riconoscimento facciale negli spazi pubblici, sia *ex post* che in tempo reale, al Parlamento Europeo nell'ottobre 2021, che ha delineato la situazione attuale dell'Unione Europea in merito all'impiego di TRF. Lo studio riporta come su 27 stati membri 11 stiano impiegando tali tecnologie, mentre altri 8 stanno organizzando i loro sistemi per procedere con la loro adozione. Più precisamente emerge come la polizia in Austria, Finlandia, Francia, Germania, Grecia, Ungheria, Italia, Lettonia, Lituania, Slovenia e Paesi Bassi impiega tecnologie di riconoscimento facciale per l'identificazione *ex post* nelle proprie indagini penali. Croazia, Cipro, Cechia, Estonia, Portogallo, Romania, Spagna e Svezia dovrebbero presto adottare la stessa tecnologia nei loro protocolli.[191]

[190] Nicolas Kayser-Bril, «At least 11 police forces use face recognition in the EU, AlgorithmWatch reveals», *AlgorithmWatch* (blog), 18 giugno 2020, https://algorithmwatch.org/en/face-recognition-police-europe/.

[191] Francesco Ragazzi et al., «Biometric & Behavioural mass surveillance in EU member states» (The Greens/EFA in the European Parliament, ottobre 2021), 19–20, https://www.greens-efa.eu/biometricsurveillance/.

Diversi paesi si sono cimentati nello scorso decennio nell'attuazione di progetti pilota, limitati nel tempo e nello spazio, per l'applicazione di sistemi di identificazione biometrica da remoto. Tra questi vale la pena ricordare:

1. Il progetto pilota, "*Safety Station Südkreuz*", attuato in Germania nel 2017 dal Ministro dell'Interno, Thomas de Maizière, che vede la collaborazione della polizia federale tedesca e della compagnia ferroviaria tedesca, per l'impiego di TRF nella stazione *Berlin Südkreuz*. Per sperimentare il sistema, il ministro ha reclutato 300 volontari che hanno acconsentito all'inserimento del proprio nome e di due foto biometriche in un database; in cambio è stato consegnato loro un voucher Amazon di 25€. Ai partecipanti è stato richiesto di portare con sé un *trasponder* in modo da permettere alle autorità di tracciare quando questi viaggiassero per la stazione. Successivamente il test prevedeva che le videocamere individuassero i comportamenti sospetti.

   Tale progetto non è risultato indenne da critiche: assenza di trasparenza e un'invasione di privacy di coloro i quali entrano in contatto con il sistema, il tutto reso più rischioso dalla preesistenza di alcuni dati nei database, sono i punti che sono stati principalmente denunciati. A condizionare ancor di più il rifiuto da parte della popolazione tedesca ha influito inoltre il *background* particolare che si porta dietro la società in Germania, che ha visto la propria sottoposizione a due regimi di sorveglianza durante il ventesimo secolo: il governo nazista prima e quello comunista poi.[192]

   Ma il paese ha visto la sperimentazione anche di altri progetti, basati sull'implementazione di software di riconoscimento facciale, per testare la capacità di rilevare comportamenti sospetti nelle città di Amburgo, Berlino e Mannhein.
2. In Francia, le autorità di Nizza, durante il carnevale del 2018, hanno condotto un test, sottoponendo un'area a sistemi di videosorveglianza dal vivo, in grado di riconoscere i volti dei passanti presenti nella *watchlist*, costituita da volontari. La città ha deciso inoltre di sottoporre a tale tecnologia anche gli alunni delle scuole superiori, con il risultato di agire in modo illegale. Ciò che ne è conseguito è stata la messa al bando del sistema negli istituti.

[192] «Big Brother in Berlin», POLITICO, 13 settembre 2018, https://www.politico.eu/article/berlin-big-brother-state-surveillance-facial-recognition-technology/.

3. Anche il Belgio si è cimentato in un progetto pilota volto a testare il sistema di riconoscimento facciale dal vivo, che ha avuto luogo nell'aeroporto internazionale di Bruxelles. Il paese rientra tra quelli, come la Spagna, che non hanno approvato l'uso di tale tecnologia, né per le indagini criminali né per la sorveglianza di massa. Nonostante tale interdizione, la polizia sta adoperando affinché anche le autorità statali agiscano al fine di lasciar cadere il divieto. Il test effettuato all'aeroporto si basa sull'impiego di quattro telecamere, connesse al software di riconoscimento facciale ad uso della polizia aeroportuale. Tale progetto, della durata di qualche mese, è stato però interrotto perché, secondo quando stabilito dal *Police Information Control Body* (COC), sarebbe stato attuato in violazione della legge belga.[193]

Sono stati condotti altri progetti pilota, come in Ungheria o in Olanda, ma la maggior parte di questi è stata dismessa.

I diversi sistemi di sorveglianza biometrica, sia in tempo reale che *ex post*, testati dagli stati, sembrano operare in una sorta di "zona grigia", dove lo sviluppo e l'impiego di queste tecnologie è nascosto alla generale visibilità. Dunque, in assenza di controllo da parte delle autorità, ciò che ne consegue è il verificarsi del rischio maggiormente temuto da coloro i quali sono contrari all'impiego di TRF negli spazi pubblici: la normalizzazione della sorveglianza. Percorrendo tale via, l'originario obbiettivo di monitorare dei comportamenti sospetti, avrà delle ripercussioni sulle libertà individuali delle persone: queste essendo a conoscenza della presenza di videocamere, potrebbero non sentirsi libere nell'esercizio dei proprio diritti fondamentali, così come garantiti dalla Carta dei diritti fondamentali dell'Unione Europea.[194] Su questa linea si è posta anche l'*European Digital Rights* (EDRi), un'associazione volta alla tutela dei diritti civili e umani, la quale il 13 maggio 2020 ha presentato una petizione alla Commissione Europea, con l'obbiettivo di richiedere

[193] Anonym, «Belgian Police Stop Facial Recognition at Zaventem Airport | Tellerreport.Com», 21 settembre 2019, https://www.tellerreport.com/tech/2019-09-21---belgian-police-stop-facial-recognition-at-zaventem-airport-.BkEeQN8QDH.html; Dominique Deckmyn e Nikolas Vanhecke, «De camera ziet u, maar wilt u ook herkend worden?», De Standaard Mobile, 12 ottobre 2019, https://www.standaard.be/cnt/dmf20191011_04658473; Ragazzi et al., «Biometric & Behavioural mass surveillance in EU member states», 9–12.

[194] «Studio Verdi, riconoscimento facciale già in uso in 11 Stati membri - Europa», ANSA.it, 29 ottobre 2021, https://www.ansa.it/europa/notizie/sviluppo_sostenibile_digitale/2021/10/29/studio-verdi-riconoscimento-facciale-gia-in-uso-in-11-paesi-ue_d6d3759e-e86c-400a-ab3b-e9aefcfdb5b8.html.

la fine di usi indebiti o arbitrari di tali tecnologie da parte di enti pubblici o privati, in quanto violano la legge UE, il GDPR e la LED, sulla protezione dei dati personali e risultano intrusivi e dunque lesivi delle libertà fondamentali, quali la privacy, il diritto alla libertà di parola, di protesta e di non discriminazione.[195] EDRi, assieme ad altre numerose associazioni che tutelano i diritti fondamentali, supporta anche la campagna *Reclaim Your Face*, volta alla raccolta di almeno un milione di firme, per l'emanazione di una legge in UE, che vieti la sorveglianza biometrica di massa: attualmente la petizione ha raccolto quasi 68000 firme.[196] Significative appaiono dunque le parole usate da Ioannis Kouvakas, Legal Officer presso Privacy International[197] e membro EDRi, secondo cui "The introduction of facial recognition into cities is a radical and dystopic idea which significantly threatens our freedoms and poses fundamental questions about the kind of societies we want to live in. As a highly intrusive surveillance technique, it can provide authorities with new opportunities to undermine democracy under the cloak of defending it. We need to permanently ban its roll out now before it's too late".

3.6 Il caso italiano: S.A.R.I.

Come nel resto dell'Unione, anche l'Italia si è cimentata nella sperimentazione di un programma per il riconoscimento facciale. Nel 2017 infatti, il Ministero dell'Interno ha adottato un Sistema Automatico di Riconoscimento delle immagini (S.A.R.I.), basato sul funzionamento di due algoritmi di elaborazione delle immagini, in grado di analizzare foto e video per permettere il riconoscimento automatico dei volti in diversi scenari. I due algoritmi, *Parsec*, creato da una società italiana, e *Neurotechnology*, da una società inglese, possono essere usati, contestualmente o separatamente: sono in grado di confrontare contemporaneamente fino a 850 elementi caratteristici, i

[195] «Ban Biometric Mass Surveillance!», European Digital Rights (EDRi), 13 maggio 2020, https://edri.org/our-work/blog-ban-biometric-mass-surveillance/.

[196] «Reclaim Your Face: Vietiamo La Sorveglianza Biometrica Di Massa!», Reclaim Your Face, consultato 4 febbraio 2022, https://reclaimyourface.eu/it/.

[197] «Privacy International è un'associazione che ha l'obbiettivo di proteggere la democrazia, difendere la dignità delle persone, e richiede alle istituzioni di assumersi la responsabilità per la violazione della fiducia pubblica, https://privacyinternational.org/about.

cosiddetti "punti fiduciari", nel momento in cui vanno ad analizzare l'immagine di un volto, posto in visione frontale.[198]

La tecnologia in uso nel paese è molto simile a quella utilizzata dalla polizia di *South Wales*, prima in Europa ad aver adottato un sistema di riconoscimento facciale. Questo è costituito da due diverse versioni:

1. SARI *Real Time* ha l'obbiettivo di offrire una funzione di supporto a operazioni di controllo sul territorio in occasione di eventi e manifestazioni: le immagini dei volti in questione, riprese in tempo reale, vengono confrontate con quelle delle persone presenti in una banca dati ristretta e predefinita, *watchlist*, creata in corrispondenza dell'evento in questione. Tale *watchlist* può essere arricchita anche con immagini prese dal web, come le foto presenti nei Social Network. Nel caso di *match positivo*, il sistema genera un *alert* che richiama gli operatori.
2. SARI *Enterprise* invece è un sistema che confronta le immagini raccolte con quelle presenti nel sistema A.F.I.S. (Automated Fingerprint Identification System), un sistema automatizzato di identificazione delle impronte digitali, banca dati centrale delle identità, che risulta essere un'evoluzione del sistema S.S.A. (Sottosistema anagrafico), che integra l'AFIS con circa una decina di milioni di foto segnaletiche con le relative informazioni anagrafiche e descrittive. Ha una finalità investigativa ed è in grado di ricercare il volto di un soggetto presente in un'immagine. Nonostante la base di ricerca si collochi nell'A.F.I.S., esso potrebbe fondarsi anche su altre banche dati, quali l'EURODAC. Il sistema è configurato in modo che all'utente siano mostrati circa 50 volti simili trovati, sarà poi il responsabile a valutare quale sia il candidato che corrisponde all'immagine in questione. Ciascuna foto indica la percentuale di somiglianza: più questa è tendente a 100% più sarà possibile l'identità tra le due immagini e se il sistema indica 100%, si avrà un giudizio

[198] Roberto V.O. Valli, «Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini», *il Penalista*, 16 gennaio 2019, https://ilpenalista.it/articoli/focus/sullutilizzabilit-processuale-del-sari-il-confronto-automatizzato-di-volti; Giorgia Pacino, «Come funziona Sari, il sistema di riconoscimento facciale usato dalla Polizia scientifica», *la Repubblica*, 7 settembre 2018, https://www.repubblica.it/cronaca/2018/09/07/news/come_funziona_sari_il_sistema_di_riconoscimento_facciale_usato_dalla_polizia_scientifica-205804445/.

di identità tra candidato e la persona la cui identità è stata sottoposta a confronto.

L'utilizzo di tali strumenti ha suscitato fin dal momento della loro realizzazione forti perplessità in merito al fondamento legislativo di tali sistemi, che per molti sembra essere quasi totalmente assente: il loro utilizzo viola, primo tra tutti, il diritto di privacy, in quanto realizzerebbe, per come è stato progettato, una forma di sorveglianza di massa.

In merito a tali due strumenti è intervenuto il Garante per la protezione dei dati personali. In un parere del 27 luglio 2018 si è pronunciato su SARI *Enterprise*, reputando che "il trattamento di dati personali da realizzarsi mediante il sistema SARI Enterprise, secondo i presupposti descritti, non presenta criticità sotto il profilo della protezione dati": questo perché il nuovo strumento non va ad effettuare elaborazioni aggiuntive, ma si limita ad automatizzare, mediante un algoritmo, alcune operazioni che prima richiedevano l'inserimento da parte dell'operatore, come accade per i connotati identificativi. Perciò non emerge un nuovo trattamento di dati, ma piuttosto "una nuova modalità di trattamento dei dati biometrici" disciplinata dalla normativa vigente. L'utilizzo di SARI *Enterprise*, dunque, non si pone in violazione della legislazione vigente, la quale rispetta le normative presenti nel decreto del Ministro dell'Interno 24 maggio 2017, in specifico nella scheda n. 19 allegata[199], così come richiesto dal d. lgs. 18 maggio 2018, n. 51[200] in attuazione della direttiva 2016/680/UE, sulla protezione dei dati personali nei confronti dell'uso da parte della polizia.[201]

Per quanto riguarda invece l'impiego di SARI *Real time*, la versione della tecnologia di riconoscimento facciale che sfrutta l'identificazione in tempo reale, il Garante della privacy si è espresso in modo negativo, in un parere del 25 marzo 2021.

[199] «Decreto 24 maggio 2017, Ministro dell'Interno».

[200] «D. lgs. 18 maggio 2018, n. 51, Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.» (s.d.).

[201] «Sistema automatico di ricerca dell'identità di un volto» (GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 26 luglio 2018), https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9040256.

Tale provvedimento ha visto dei ritardi nella sua adozione, per la mancanza di risposte alle richieste di informazioni che il Garante privacy ha rivolto al Viminale: dopo l'apertura dell'istruttoria sul sistema SARI *Real Time* nel 2017, la corrispondenza si è interrotta nell'ottobre 2018, a seguito della richiesta di una valutazione di impatto sulla privacy dei cittadini, che risulta necessaria nel momento in cui si vanno ad adottare tecnologie che possono ledere i diritti fondamentali dei cittadini.[202] Nel provvedimento adottato dal Garante, si evidenza come il sistema non sia conforme alla disciplina contenuta negli artt. 5 e 7 del decreto legislativo 18 maggio 2018 n. 51 (attuativo della direttiva UE sulla protezione dati personali 2016/680/UE), secondo la quale il trattamento dei dati personali ad opera di organi di polizia deve essere disposto da fonte normativa, nel rispetto dei diritti fondamentali sanciti dalla CEDU, dalla Carta dei diritti fondamentali dell'Unione Europea e dal GDPR e deve secondo determinate condizioni, tra cui la previsione di fondamento normativo. Inoltre "il sistema, oltre ad essere privo di fondamento legislativo che legittimi il trattamento automatizzato dei dati biometrici per il riconoscimento facciale a fini di sicurezza, realizzerebbe per come è progettato una forma di sorveglianza indiscriminata/di massa". Il sistema, permettendo di analizzare in tempo reale i volti di soggetti ripresi attraverso dei sistemi di videosorveglianza posizionati in un determinato territorio e confrontandoli con quelli presenti in una banca dati, violerebbe il diritto alla riservatezza, visto l'utilizzo di dati sensibili. Ciò che emerge sarebbe dunque la realizzazione di un trattamento automatizzato su larga scala che, coinvolgerebbe anche coloro i quali partecipano a manifestazioni politiche e sociali, nonostante la loro persona non risulta essere oggetto di "attenzione" da parte delle forze di polizia. Pertanto, secondo la posizione espressa dal Garante il sistema SARI *Real Time* non può essere utilizzato come supporto all'attività di contrasto.[203]

In generale si può constatare che la criticità maggiormente evidenziata si fonda sul fatto che le due tecnologie, in assenza di un fondamento normativo, potrebbero venir usate dalla polizia in circostanze e per finalità molto diverse, ponendo a rischio il rispetto del principio di proporzionalità: il loro utilizzo può accadere per esempio

[202] Riccardo Coluccini, «Lo scontro Viminale-Garante della privacy sul riconoscimento facciale in tempo reale», *IrpiMedia* (blog), 13 gennaio 2021, https://irpimedia.irpi.eu/viminale-garante-privacy-riconoscimento-facciale-in-tempo-reale/.

[203] «Parere sul sistema Sari Real Time» (GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 25 marzo 2021).

nell'impiego di sistemi di videosorveglianza degli stadi, dove non si procede al confronto mirato di determinati soggetti, con foto contenute in database, ma piuttosto si cerca di identificare le persone tra la folla, mediante la comparazione con immagini presenti in tali banche dati.[204]

L'adozione di tali sistemi ha portato anche il legislatore ad assumere posizioni divergenti, tanto che ci sono state degli atti di sindacato ispettivo in Parlamento volte a chiedere chiarimenti al Ministro dell'Interno, al fine di evidenziare la necessità di una moratoria dell'impiego di sistemi di videosorveglianza per predisporre una normativa privacy adeguata, che vada a tutelare i diritti costituzionali dei cittadini.[205]

A seguito di tali atti, il 12 aprile 2021, un gruppo di deputati ha presentato una proposta di legge per la "Sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici in luoghi pubblici o aperti al pubblico". In merito a tale disegno, la Commissione affari costituzionali, in data 10 novembre 2021, ha svolto l'audizione del responsabile dell'*AlgoritmWatch* (impegnata nel monitoraggio di sistemi decisionali automatizzati e nel loro impatto nella società), Fabio Chiusi, il quale ha illustrato le problematicità dell'utilizzo di tali tecnologie. Nella sua audizione l'esperto ha delineato come la previsione di una moratoria, in attesa dell'emanazione di un complesso normativo sulla privacy che vada a garantire la protezione dei diritti costituzionali, non sia sufficiente, ma piuttosto sia necessario procedere alla messa al bando di tali tecnologie, in quanto contrastanti con i principi che caratterizzano una società democratica. Ciò che appare davvero importante però, consta del fatto che non sono solo i sistemi di videosorveglianza in tempo reale che devono essere vietati, ma anche quei sistemi che permettono un riconoscimento delle immagini *ex post*, attraverso il *matching*, come dimostra il caso della famosa app Clearview AI. Fabio Chiusi dichiara che nonostante l'art. 1 di tale disegno di legge sancisca il divieto di installazione e utilizzazione di impianti di videosorveglianza, appare fondamentale imporre un divieto *ex ante*, che vada ad impedire l'immissione nel mercato di tali

[204] «Sistema di videosorveglianza presso lo Stadio Olimpico. Verifica preliminare» (GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 28 luglio 2016), https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/5386852.

[205] «XVIII legislatura, Interpellanza urgente 2/01109» (CAMERA DEI DEPUTATI, 22 febbraio 2021), https://www.camera.it/leg18/1; «Interrogazione a risposta immediata in Assemblea 3/02074» (CAMERA DEI DEPUTATI, 3 marzo 2021).

tecnologie, onde evitare che possano ripetersi episodi come quello che ha coinvolto la città di Udine. In questo caso la città ha investito nell'acquisto di un gran numero di strumenti per la videosorveglianza da installare nelle vie della città, ma il loro utilizzo è stato impedito dal divieto che la normativa vigente ha imposto. Lapalissiano appare dunque il risultato che si sarebbe ottenuto se la legge avesse previsto un divieto *ex ante*, che impedisse l'acquisto della tecnologia: la città avrebbe potuto investire in modo più efficiente i soldi spesi per offrire dei servizi migliori alla società, senza causare così uno spreco ingiustificato di denaro pubblico.

Il Garante per la protezione dei dati personali italiano, dopo aver eseguito un'istruttoria, attivata a seguito di reclami e segnalazioni, il 9 marzo 2022 è intervenuto in merito al programma Clearview AI, assumendo una posizione simile a quella francese: ha imposto alla società una sanzione di 20 milioni di euro, per aver messo in atto un vero e proprio monitoraggio biometrico anche di persone che si trovano nel territorio italiano, e ha ordinato la cancellazione dei dati relativi ai soggetti che si trovano in Italia. Ulteriore imposizione stabilita consiste nella designazione di un rappresentante nel territorio dell'Unione Europea che funga da interlocutore, in aggiunta o in sostituzione del titolare del trattamento dei dati con sede negli Stati Uniti, al fine di agevolare l'esercizio dei diritti degli interessati.[206]

Ma anche altre città italiane si sono cimentate nell'uso di tecnologie di riconoscimento facciale. Spicca il caso della città di Como, la quale, a seguito di disordini sorti nel 2016 a causa delle rotte migratorie verso nord, che hanno visto il paese come snodo, ha deciso di installare nell'agosto 2019 delle telecamere con funzioni di video sorveglianza nella zona del parco di via Tokamachi, che permettono il riconoscimento facciale e la visualizzazione in tempo reale di immagini. In merito all'installazione si è espresso negativamente il Garante della Privacy, con un parere del 26 febbraio 2020, il quale ha evidenziato come l'impiego di tali sistemi volti al riconoscimento dei volti in tempo reale non sia conforme alle norme giuridiche e ne sia sprovvisto di fondamento.[207]

[206] «Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani», Garante Privacy, 9 marzo 2022, https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9751323.

[207] «Provvedimento del 26 febbraio 2020» (GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 26 febbraio 2020), https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9309458.

Successivamente il 1° dicembre 2021 il Parlamento ha votato favorevolmente un emendamento all'art. 9 del d.l. 139/2021, noto come decreto Capienze, che è stato convertito in legge, l. 205 del 3 dicembre 2021[208], con la quale si inserisce una nuova norma che prevede una moratoria di due anni, che decorre dal momento in cui entra in vigore questa legge e ha scadenza il 31 dicembre 2023 che va a sospendere l'uso di sistemi di riconoscimento facciale, sia da parte di autorità pubbliche che di privati. Il co. 12 dell'art. 9 sancisce che rimane salva la possibilità di uso di questi sistemi a fini di prevenzione e repressione delle sanzioni penali di cui al d. lgs. n. 51/2018, in presenza, se autorizzate dalla magistratura. In posizione contraria a tale norma, in linea anche con quanto stabilito dall'associazione *AlgorithmWatch*, si posiziona l'associazione *Privacy Network*, la quale seppur riconosce l'importanza di un tale traguardo, evidenzia come la moratoria non va a colpire la maggior parte degli utilizzi di tali tecnologie, ovvero reprimere e prevenire reati, in quanto tale categoria risulta essere esclusa. Le novità introdotte dunque hanno un'incidenza molto ridotta. Il modo in cui si è deciso di disciplinare la materia conduce però ad un effetto indesiderato e contrario all'obbiettivo iniziale, in quanto disciplinando con legge i possibili utilizzi di tali tecnologie, si è ottenuto il risultato di agevolare l'uso di sistemi di riconoscimento facciale per finalità di repressione e prevenzione di reati, con la conseguenza di rendere lecito il loro utilizzo.[209] Ioannais Kouvakas, membro dell'ufficio legale di *Privacy International*, in un'intervista a *Wired*, ha commentato dichiarando che tali fenomeni conducono proprio alla creazione di una società costantemente sorvegliata: emergono non solo implicazioni per la privacy, ma anche aspetti etici connessi al fatto che una società democratica non può ammettere l'utilizzo di una tecnologia così intrusiva. A ciò si aggiunge che tali sistemi vengono utilizzati in assenza di trasparenza e giustificazioni adatte, violando dunque le normative per la tutela dei diritti umani.[210]

[208] «L. 3 dicembre 2021 n. 205, Conversione in legge, con modificazioni, del decreto-legge 8 ottobre 2021, n. 139, recante disposizioni urgenti per l'accesso alle attivitaà culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali» (s.d.).

[209] «Italia - Moratoria sul riconoscimento facciale», *Privacy Network* (blog), 2 dicembre 2021, https://www.privacy-network.it/iniziative/italia-moratoria-sul-riconoscimento-facciale/.

[210] Riccardo Coluccini, Laura Carrer, e Philip Di Salvo, «Perché Como è diventata una delle prime città in Italia a usare il riconoscimento facciale», *Wired Italia*, 9 giugno 2020, https://www.wired.it/internet/regole/2020/06/09/riconoscimento-facciale-como/.

4. STATI UNITI

4.1 La mancanza di una regolamentazione a livello federale

Gli Stati Uniti nel 1791 approvano i dieci emendamenti alla Costituzione Americana, noti anche con il nome di Bill of Rights, che rappresentano garanzie fondamentali per le libertà, la giustizia e i diritti civili nei confronti del governo. Ma sebbene il paese da sempre sia stato considerato la "patria delle libertà", sembra che con l'avvento della tecnologia tale appellativo non risulti più descrivere la realtà sociale: l'intromissione nelle vite private che tali strumenti permettono di compiere sta realizzando sempre più quel modello di società, tanto scongiurata, costantemente posta sotto l'occhio del Grande Fratello.

Dal 2013 al 2019 le richieste del governo ai grandi Big Tech, in merito ai dati da questi tenuti, sono aumentate del 213% (anche se fortunatamente vengono soddisfatte in parte, dal 55% al 75%): ciò significa che le persone non si devono preoccupare semplicemente di come i grandi produttori di IT acquisiscano o utilizzano le nostre informazioni, ma soprattutto di come siano cedute ai governi, in grado così di realizzare la tanto temuta sorveglianza generalizzata, resa possibile dai poteri in capo a questi. Tale aumento probabilmente è dipeso dagli scandali che hanno interessato la National Security Agency (NSA), organismo del dipartimento di difesa degli USA che, assieme all'FBI e alla CIA, si occupa della sicurezza nazionale. La vicenda ha interessato le rivelazioni che Edward Snowden ha diffuso, riguardati l'uso dei dati personali che le maggiori agenzie dell'USA han impiegato.[211] A ciò è susseguito poi un ulteriore episodio di non meno risonanza mediatica, che ha interessato anche l'UE, riguardante la presa consapevolezza della possibile strumentalizzazione dei propri dati personali. I protagonisti dello scandalo sono Facebook e la società di consulenza britannica Cambridge Analytica: quest'ultima ha collezionato i dati degli utenti del grande colosso dei Social Network, senza il loro consenso, al fine di impiegarli per scopi di propaganda politica.[212]

È probabilmente a seguito di queste due rivelazioni, rese note alla popolazione, che hanno iniziato a manifestarsi le prime preoccupazioni in merito alla crescente

---

[211] Pijus Jauniškis, «How Do I Know If the Government Is Watching Me?», Surfshark, 3 novembre 2021, https://surfshark.com/blog/is-the-government-watching-me.

[212] Karim Amer e Jehame Noujaim, *The Great Hack - Privacy violata*, 2019.

evoluzione dell'intelligenza artificiale, in grado di raggiungere prestazioni sempre più simili a quelle di pertinenza dell'intelligenza umana.

Seppur gli Stati Uniti risultino leader nello sviluppo dell'intelligenza artificiale, grazie alla presenza in suolo americano, in modo particolare nella Silicon Valley, dei maggior Big Tech, alla ricerca costante di nuove tecnologie sempre più performanti, non si riscontra ancora una legislazione a livello federale che regolamenti tali innovazioni. Specificamente non è presente alcuna regolamentazione dei sistemi di riconoscimento facciale a livello federale, sebbene non manchi l'impegno del mondo politico nella presentazione di progetti di normazione che disciplinino tale tecnologia così innovativa, ma non priva di conseguenze negative, come già precedentemente riportato, che meritano, proprio per questo motivo, controllo e uniformità nell'impiego.

Nel giugno 2021 è stato presentato infatti un disegno di legge, il *Facial Recognition and Biometric Technology Moratorium Act*[213], da una coalizione di politici appartenenti all'ala democratica, tra cui emergono i nomi di Elisabeth Warren e Bernie Sanders, volto a regolare l'impiego degli strumenti da parte delle forze dell'ordine. Il progetto, che non ha ancora passato il vaglio del Congresso, prende a riferimento la proposta di legge *No Biometric Barries Housing Act*[214] del 2021, già presentata nel 2019 e reiterata lo scorso anno, il cui intento è l'introduzione di un divieto dell'uso di TRF nelle unità abitative pubbliche e assistite, finanziate dal dipartimento per gli alloggi e lo sviluppo urbano. La proposta presentata dai democratici sancisce un divieto per l'acquisto di qualsiasi strumento di identificazione biometrica, fornendo inoltre un diritto di azione privata a chiunque subisca l'impiego delle proprie informazioni personali in violazione delle norme. Le normative statali o locali che già regolano la materia non verrebbero abrogate dall'emanazione di tale nuova legge, ma questa condizionerebbe il finanziamento delle sovvenzioni federali a porre moratorie su di esso.[215]

[213] «Facial Recognition and Biometric Technology Moratorium Act of 2021» (2021).

[214] «No Biometric Barries Housing Act» (2021).

[215] Scott Ikeda, «Maine Becomes First State To Pass Broad Government Ban on Facial Recognition Technology», CPO Magazine, 8 luglio 2021, https://www.cpomagazine.com/data-privacy/maine-becomes-first-state-to-pass-broad-government-ban-on-facial-recognition-technology/.

Attualmente l'impiego della tecnologia manca di una disciplina omogenea in grado di garantire il rispetto del diritto di uguaglianza e di non discriminazione in tutti gli stati degli USA. Si assiste perciò all'emanazione di una pluralità di norme che caratterizzano in modo diverso alcune città o anche stati: si genera così un'eterogeneità normativa nel paese. Le leggi che sembrano riscuotere la maggior condivisione sono quelle che si pongono proprio l'obbiettivo di regolare in modo uniforme la materia, senza incorrere in un divieto assoluto o in un "liberi tutti", che conduce rispettivamente da un lato al venir meno di quei benefici che si possono trarre dall'utilizzo di questa tecnologia, quali il miglioramento della vita e la sicurezza della persone, ma dall'altro se non disciplinati rischiano il perpetuarsi di abusi, in modo particolare da parte delle forze dell'ordine, come si è potuto constatare nei diversi episodi che hanno caratterizzato gli Stati Uniti nell'arresto di persone appartenenti alla comunità nera.

L'impiego di TRF probabilmente non verrà messo completamente al bando dalla legislazione statunitense, dal momento che la posizione che sembra assumere il Congresso appare più moderata, cosciente del fatto che sottrarre tale tecnologia all'attività delle forze dell'ordine significa togliere risorse importanti alla sicurezza nazionale. Il *Center For Strategic & International Studies*, un centro studi fondato dalla Georgetown University, in un report pubblicato nel settembre 2021, ha infatti esposto delle linee guida per l'emanazione di una disciplina normativa che regolamenti l'impiego di tali strumenti, sfruttandone le potenzialità in modo etico e legale. Fondamentale per l'uso lecito, secondo gli autori, appare essere: la previsione di un numero limitato di soggetti che possano accedere a tali sistemi, superando così la frammentarietà della regolazione degli stati e prevedendo delle norme che rispettino i diritti e le libertà civili; la restrizione dell'uso, stabilendo dunque le circostanze in cui i soggetti abilitati possono impiegare tali software; la trasparenza nell'installazione delle TRF, rendendo noto al pubblico il modo in cui funzionano; la protezione del soggetto dagli errori che l'algoritmo può commettere nell'individuare la persona in questione, garantendo la revisione delle corrispondenze restituite dal software di riconoscimento facciale; la disciplina chiara della raccolta e della conservazione dei dati, che preveda l'utilizzo solo nei casi consentiti; espressione del consenso nei casi in cui uno specifico uso lo richieda, come nel caso in cui sia necessario un mandato; la garanzia di un controllo umano in merito ai risultati ottenuti dal software; e infine il

continuo aggiornamento della tecnologia sulla base dei progressi informatici raggiunti.[216]

Precedentemente, nel dicembre 2020, già un altro studio, *Biometric face recognition: references for policymaker*, ha elaborato un documento volto a fornire ai politici statunitensi un quadro completo della tecnologia di identificazione biometrica, al fine di permettere loro di promuovere una normativa fondata su una conoscenza a tutto tondo sul sistema di funzionamento, su criticità e potenzialità, sulla possibilità di intervento in aree di attività. Tale report offre le linee guida molto simili a quelle riproposte dallo studio successivo realizzato dal *Center For Strategic & International Studies*.[217]

Sebbene tale disciplina normativa non sia tutt'ora presente, non mancano però azioni intraprese da alcuni organi pubblici volti a delineare alcuni principi etici da adottare nel caso di uso dell'intelligenza artificiale. Tra questi vi è il dipartimento della Difesa, che, il 24 febbraio 2020, dopo 15 mesi di collaborazione con il governo, il settore commerciale e l'università, per l'analisi di tali strumenti, ha adottato delle raccomandazioni con l'obbiettivo di affrontare in modo appropriato ed etico le sfide si presentano, garantendo però contemporaneamente l'uso responsabile dell'AI.[218]

La diffusione di tale strumento ha interessato anche molte associazioni che si battono da anni per la tutela dei diritti civili: è proprio nella patria dei diritti che si assiste al moltiplicarsi di campagne volte a promuovere il divieto della tecnologia di riconoscimento facciale.

Tra queste vi è la petizione *Ban the scan* di Amnesty International, che chiede la messa al bando di qualsiasi TRF, in quanto considerata invadente, oppressiva e razzista. L'associazione sostiene che tali strumenti violano costantemente il diritto alla privacy, minacciando i diritti alla libertà di riunione, di espressione pacifica, all'uguaglianza e alla non discriminazione, in quanto i grandi Big Tech, creatori di tali

[216] James A. Lewis e William Crumpler, «Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape», 29 settembre 2021, https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape.

[217] «Biometric face recognition: references for policymaker - An informational document created by the fedid comunity» (Federal Identity Community (FedID) Cmmunity, dicembre 2020).

[218] «DOD Adopts Ethical Principles for Artificial Intelligence», U.S. Department of Defense, 24 febbraio 2020, https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

software, costituiscono database prendendo le nostre informazioni più personali e sensibili dal web, in totale assenza del nostro consenso e a nostra insaputa. Ma ciò che, secondo Amnesty International, risulta ancor più pericolosa è l'imprecisione che accumuna la maggior parte di tali tecnologie, capace di raggiungere un livello di non accuratezza del 95%. La posizione assunta ha condotto a promuovere sia una petizione specificamente per la città di New York, ma anche, più in generale, una campagna globale rivolta non solo al mondo statunitense, ma alla totalità dei paesi nel mondo.[219]

L'*Electronic Privacy Information Center* (EPIC), un gruppo di ricerca pubblico statunitense, con sede a Washington, ha promosso un'altra campagna volta a promuovere il divieto dell'uso di TRF da parte delle forze dell'ordine. L'organizzazione invita a riflettere sulla pericolosità del sistema, dipesa dal fatto che la tecnologia che sta diffondendosi largamente consente l'identificazione segreta e persino remota su larga scala. EPIC pone l'attenzione sulle azioni che ciascuno stato dovrebbe compiere: innanzitutto è necessario procedere alla sospensione dell'ulteriore diffusione di tali strumenti; consegue il valutare se i dati costituenti i database siano stati ottenuti legalmente, cancellando nel caso quelli ottenuti in modo illegale; poi bisogna intraprendere studi volti a valutare i pregiudizi, la privacy e la protezione dei dati e le implicazioni sociali e etiche; infine sono necessarie delle regole legali, standard tecnici e linee guida etiche per la salvaguardia dei diritti fondamentali.[220]

Un'ulteriore, ma non ultima, petizione è stata promossa da *Fight for the Future*, un gruppo di difesa senza scopo di lucro nel settore dei diritti digitali fondato nel 2011,[221] sulla convinzione che il riconoscimento facciale sia "unreliable, unjust, and a threat to basic rights and safety". La campagna promossa vede la partecipazione di moltissime associazioni impegnate quotidianamente nella lotta per la salvaguardia dei diritti, quali Greenpeace, EPIC, ACLU e molte altre. Secondo la posizione assunta i

[219] «Ban the scan - New York City», *Amnesty International* (blog), consultato 5 marzo 2022, https://banthescan.amnesty.org/nyc/; «Ban the scan», Amnesty International, consultato 5 marzo 2022, https://banthescan.amnesty.org/; «Polizia di New York, parte dagli USA la campagna per evitare i sistemi di riconoscimento facciale: "Amplificano il razzismo della polizia"», la Repubblica, 26 gennaio 2021, https://www.repubblica.it/solidarieta/diritti-umani/2021/01/26/news/profughi-284302004/.

[220] «Ban Face Surveillance», *EPIC - Electronic Privacy Information Center* (blog), consultato 10 febbraio 2022, https://epic.org/campaigns/ban-face-surveillance/.

[221] «Fight for the Future», in *Wikipedia*, 23 gennaio 2022, https://en.wikipedia.org/w/index.php?title=Fight_for_the_Future&oldid=1067408560.

benefici sono ampiamente superati dalle minacce che tale sistema arreca alla società.[222]

Al centro della lotta per un divieto delle TRF si pone L'*American Civil Liberties Union* (ACLU) che nel contesto del progetto *Speech, Privacy and Technology*, si pone l'obbiettivo di tutelare l'individuo con tutti i suoi diritti, tra cui la privacy che risulta erosa dall'impiego di strumenti biometrici. A tal fine l'associazione sta lavorando con tribunali, legislature e comunità per difendere e preservare tali diritti e libertà garantiti dalla costituzione e dalle leggi negli USA. È infatti impegnata in numerose cause legali che denunciano l'uso improprio che forze dell'ordine, fornitori commerciali di software e governi stanno compiendo, con il rischio di creare la società, tanto temuta, sottoposta a costante sorveglianza di massa.[223]

4.2 Il Maine: il primo stato a regolare la legislazione sul riconoscimento facciale

Negli Stati Uniti si è assistito negli ultimi anni all'emanazione di una serie di atti volti a vietare o limitare l'uso della tecnologia di riconoscimento facciale limitatamente ad alcune città del paese, rivolgendo dunque le restrizioni a piccoli gruppi nei diversi stati. Fino ad ora però non si era mai verificata la previsione a livello statale di una regolamentazione *ad hoc*, per quanto attiene l'impiego di tecnologia in questione: il Maine è il primo stato negli USA ad aver emanato una legge che prevede il divieto delle TRF nella maggior parte degli usi governativi. Il progetto di legge, *An Act To Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials*, presentato alla Camera il 28 aprile 2021 dal democratico Grayson Locker, membro della camera dei rappresentanti del Maine, e convertito in legge il primo luglio, è entrata in vigore lo scorso primo ottobre.[224]

[222] «Ban Facial Recognition», Ban Facial Recognition, consultato 7 marzo 2022, https://www.banfacialrecognition.com.

[223] «The Fight to Stop Face Recognition Technology | News & Commentary», American Civil Liberties Union, consultato 7 marzo 2022, https://www.aclu.org/news/topic/stopping-face-recognition-surveillance/.

[224] Mike Maharrey, «Now in Effect: Maine Law Limits Government Use of Facial Recognition | Tenth Amendment Center», Tenth Amendment center, 1 ottobre 2021,

Il divieto predisposto dallo stato segue la linea assunta precedentemente dalla città di Portland, la quale ha adottato un'ordinanza per vietare l'uso della tecnologia di riconoscimento facciale nell'agosto 2020. La proposta è stata presentata dal consigliere comunale Pious Ali nel novembre 2019, ma è stata adottata, su pressione del movimento Black Lives Matter di Portland, solo a seguito della morte del giovane George Floyd a Minneapolis avvenuta nel maggio 2020.[225]

Ponendosi in modo anticipato rispetto a ipotetici progetti a livello federale, lo stato del Maine può essere considerato un esempio molto rigoroso negli USA, in grado di far cooperare e convergere verso un obbiettivo comune le diverse forze e anime presenti nel paese. Come si può constatare dal testo di legge emanato, è posto severo divieto, ai diversi livelli di stato, a dipartimenti, dipendenti e funzionari statali, di contea e municipali, di utilizzare o possedere la tecnologia di riconoscimento facciale o di stipulare un accordo con terzi per ottenere, accedere o utilizzare tali sistemi di sorveglianza o le informazioni ottenute tramite questi, nella maggior parte delle aree pubbliche, comprese le scuole, e per scopi di sorveglianza, volti a controllare incontri politici e proteste, e in generale andando ad incidere sulle libertà delle persone. A seguito di alcuni emendamenti sono state introdotte delle eccezioni, rientranti in un severo quadro regolatorio costituito da standard rigidi, che prevedono la possibilità per le forze dell'ordine di poter richiedere all'FBI e al *Maine Bureau of Motor Vehicles* una ricerca di riconoscimento facciale con "probable cause to believe an unidentified person in an image committed a serious crime" (repressione e indagini su crimini) o quando si assiste all'identificazione di una persona deceduta, scomparsa o in pericolo. I risultati di tali ricerche dovranno rimanere pubblici. La disposizione di legge prevede inoltre che i dati ottenuti con il sistema di riconoscimento facciale, quando è ammesso il suo utilizzo, non possano essi stessi fungere da unica causa di arresto; per di più se questi sono ottenuti in violazione della previsione legislativa saranno considerate prove inammissibili.

La legge in questione predispone inoltre una novità di non poco rilievo: al cittadino è garantito il diritto di azione privata nei confronti delle autorità che gli

https://blog.tenthamendmentcenter.com/2021/10/now-in-effect-maine-law-limits-government-use-of-facial-recognition/.

[225] Randy Billings, «Portland councilors approve ban on facial recognition technology», *Press Herald*, 4 agosto 2020, https://www.pressherald.com/2020/08/03/portland-councilors-approve-ban-on-facial-recognition-technology/.

garantisce adeguata tutela contro l'abuso della TRF perpetrato da parte delle forze dell'ordine, che comporta la violazione degli obblighi previsti da tale normativa.[226]

In quanto esclusivamente rivolte ai diversi livelli statali, le disposizioni contenute nella norma, in vigore dal primo ottobre, però non avranno alcuna efficacia per quanto attiene le agenzie federali che hanno sede nel paese, con ciò permettendo dunque il massivo impiego della tecnologia di riconoscimento facciale da parte di queste, vista l'assenza di una legge federale.[227]

Pertanto, al fine di rendere possibile lo sfruttamento delle potenzialità offerte da tali sistemi, lo stato del Maine ha stabilito, come requisito per un loro impiego posto a garanzia dei diritti, che le forze dell'ordine statali possano utilizzare la TRF solo se impossibilitate nell'espletamento di altri strumenti, risultando così necessario il suo uso per una corretta prosecuzione dell'indagine; inoltre i reati perseguiti devono rientrare nella categoria "*serious crime*": al fine di rendere chiara l'applicazione della norma, la legge ne predispone una definizione alla lettera I, onde evitare il sorgere interpretazioni contrastanti.[228]

L'iniziativa legislativa ha da subito ottenuto un ampio e bipartitico appoggio, che ha visto il passaggio in parlamento, attraverso l'unanimità in entrambe le camere. Ciò testimonia come il sentire comune dell'intera popolazione del Maine coincidesse proprio con quanto la legge prevede, ovvero l'esigenza di vietare l'utilizzo degli strumenti in questione per garantire i diritti del rispetto della vita privata.

Il raggiungimento dell'accordo sul contenuto della disposizione è stato ottenuto garantendo la partecipazione al tavolo di tutti coloro i quali possono avere ripercussioni o comunque un interesse rilevante nella diversa regolazione della tecnologia di riconoscimento, quali la *Maine State Police* e il *Maine Department of Public Safety*. In merito a ciò il suo principale promotore ha dichiarato infatti "I'm proud of this bill and the process it went through, which included bringing law enforcement partners to the table". Tuttavia, nonostante tale il notevole risultato, non

[226] Grace Woodruff, «Maine Now Has the Toughest Facial Recognition Restrictions in the U.S.», *Slate*, 2 luglio 2021, https://slate.com/technology/2021/07/maine-facial-recognition-government-use-law.html.

[227] «An Act To Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials'» (2021).

[228] An Act To Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials'.

sono mancate le opposizioni da parte del corpo di polizia: la *Maine Sheriff Association* ha dichiarato come le diverse lamentele presentate dagli oppositori dell'impiego della tecnologia risultano essere estremamente esagerate. Con tale regolamentazione, secondo l'associazione, si verrebbero a perdere quei benefici che l'impiego della strumentazione in questione garantisce nella lotta alla criminalità. Secondo lo sceriffo Troy Morton, infatti, risulta di fondamentale importanza mantenere in uso tale sistema per garantire la sicurezza nelle città: basti pensare che nel 2001 i terroristi che compirono l'attentato alle Torri Gemelle passarono per l'aeroporto di Portland, e se in tale occasione fosse stato possibile utilizzare la TRF, afferma lo sceriffo, si sarebbe potuta evitare la morte di 3000 persone.[229]

A sostegno di tale iniziativa si è posta sin da subito l'associazione per i diritti umani, *American Civil Liberties Union* (ACLU), che da anni si batte per promuovere la messa al bando di tali tecnologie, altamente intrusive e dunque lesive di diritti fondamentali, che hanno richiesto gran impegno e lotte sociali per il loro riconoscimento. Al centro della lotta contro l'uso massivo degli strumenti in questione, ACLU pone le discriminazioni che l'algoritmo impiegato dalla TRF genera: come riportano lo studio tenuto dai ricercatori dell'MIT[230] e quello realizzato da un'agenzia federale su circa 200 algoritmi[231], la tecnologia risulta altamente discriminatoria verso le minoranze etniche, in modo particolare verso le donne nere. L'associazione ha lavorato a stretto contatto con il promotore della legge Grayson Lookner per introdurre una disposizione che prevedesse strette limitazioni per l'impiego di TRF.[232]

"Maine is showing the rest of the country what it looks like when we the people are in control of our civil rights and civil liberties, not tech companies that stand to profit from widespread government use of face surveillance technology" afferma

[229] Scott Writer, «Lawmakers may limit use of facial recognition software by police in Maine», *Press Herald* (blog), 25 maggio 2021, https://www.pressherald.com/2021/05/25/legislature-may-limit-use-of-facial-recognition-software-by-police-in-maine/.

[230] Hardesty, «Study finds gender and skin-type bias in commercial artificial-intelligence systems».

[231] Sarah Henderson, «NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software», text, NIST, 19 dicembre 2019, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

[232] Michael Ratsimbazafy, «Maine's Landmark Facial Recognition Law: Preserving Our Rights in the 21st Century», ACLU of Maine, 2 agosto 2021, https://www.aclumaine.org/en/facial-recognition-summer-blog.

Michael Kebede, consulente politico per ACLU nel Maine.[233] Tale dichiarazione è stata rilasciata al fine di evidenziare come questa sia considerata una vittoria, la legge emanata si pone in netta contrapposizione alla quella emanata a Washington nel 2020, che predispone una regolazione dell'uso di TRF, non una messa al bando, con la conseguenza di ammettere tali strumenti quali mezzi di sorveglianza di massa.

A supporto del progetto di legge si è posta anche l'associazione non-profit *Immigrant Legal Advocacy Project*, che nel Maine offre sostegno a coloro che si trovano in difficoltà economica o che sono immigrati. Julia Brown, un suo membro, prima dell'adozione della legge, si è rivolta in un'audizione di fronte a *Criminal Justice and Public Safety Committee*, testimoniando come l'impiego di tali tecnologie sia estremamente dannoso, in modo particolare nei confronti della popolazione immigrata, che conta circa il 4% di quella totale nel Maine; inoltre, il loro impiego risulterebbe effettuato senza un previo consenso o conoscenza da parte del soggetto sottoposto al sistema. In virtù di tali criticità, secondo l'avvocato risultava necessaria l'adozione del progetto di legge presentato da Grayson Locker, volto a vietare l'utilizzo in modo diffuso della tecnologia.[234]

4.3 Diffusione del divieto dell'uso di TRF in alcune città degli USA

La regolamentazione della tecnologia di riconoscimento facciale, come riportato precedentemente, non ha interessato solo lo stato del Maine, ma ha visto una prima diffusione di divieti in molte città degli Stati Uniti, in particolar modo in alcune città del Massachusetts e della California. Generalmente nel resto delle città e degli stati degli USA invece si è disposta una regolamentazione volta a limitare in modo più debole l'utilizzo degli strumenti di identificazione biometrica, comportando così il mantenimento dei software di riconoscimento facciale in dotazione alle forze dell'ordine, purché vengano impiegati nel rispetto di alcuni standard specifici.

[233] «Maine Enacts Strongest Statewide Facial Recognition Regulations in the Country», American Civil Liberties Union, 30 giugno 2021, https://www.aclu.org/press-releases/maine-enacts-strongest-statewide-facial-recognition-regulations-country.

[234] Julia Brown, «Testimony of Julia Brown, Immigrant Legal Advocacy Project In Support of LD 1585, "An Act To Increase Privacy and Security by Prohibiting the Use of Facial Surveillance by Certain Government Employees and Officials."» (Immigrant Legal Advoct Project, 12 maggio 2021), http://www.mainelegislature.org/legis/bills/getTestimonyDoc.asp?id=164320.

Prima tra tutte ad introdurre un divieto generale negli USA è la città di San Francisco (California), che nel 2019 ha introdotto un divieto per l'impiego della tecnologia di identificazione biometrica da parte delle agenzie governative, inclusi i dipartimenti di polizia e quelli dello sceriffo di contea.[235] Ancora una volta l'ordinanza, approvata il 14 maggio 2019, ha trovato il sostegno dell'associazione ACLU of Northern California, che ha ribadito, per voce di Matt Cagle, suo esponente, come tali sistemi di riconoscimento facciale siano incompatibili con una sana democrazia.[236]

La previsione normativa non va ad interferire invece con gli usi personali, quali per esempio lo sblocco degli smartphone mediante il riconoscimento del volto. In virtù di ciò, alla polizia è ammesso l'uso di immagini provenienti da telecamere poste negli spazi privati. La previsione non si applica neppure alle agenzie federali e dunque neppure negli aeroporti e nei porti, in quanto sottoposti alla giurisdizione di queste ultime.[237] Tra le eccezioni che la regolamentazione predisposta dalla città prevede vi è inoltre quella che prevede la possibilità per pubblici ministeri di impiegare TRF nel caso in cui il requisito di trasparenza possa andare ad interferire con le loro investigazioni in corso.

Alla decisione di San Francisco di vietare le TRF non sono mancate opposizioni. Tra queste, vi è la posizione assunta dal gruppo locale *Stop Crime SF*, un'organizzazione di vicinato volta a vigilare e proteggere le abitazioni da incursioni, secondo la quale sottrarre tali strumenti rimuove un potenziale deterrente contro i crimini di proprietà, influisce sulla raccolta di prove, riducendo risorse nella ricerca di persone scomparse o vittime di traffici umani.[238] Il suo vicepresidente dichiara che, seppur tali strumenti non sono perfetti, risulterebbe più idonea l'applicazione di una

[235] Tony Raval, «Council Post: Examining The San Francisco Facial-Recognition Ban», *Forbes*, 21 giugno 2021, https://www.forbes.com/sites/forbestechcouncil/2019/06/21/examining-the-san-francisco-facial-recognition-ban/.

[236] «San Francisco Is First US City to Ban Facial Recognition», *BBC News*, 14 maggio 2019, par. Technology, https://www.bbc.com/news/technology-48276660.

[237] Gregory Barber, «San Francisco Bans Agency Use of Facial Recognition Tech», *Wired*, 14 maggio 2019, https://www.wired.com/story/san-francisco-bans-use-facial-recognition-tech/; Rachel Metz, «San Francisco just banned facial-recognition technology», CNN, 14 maggio 2019, https://www.cnn.com/2019/05/14/tech/san-francisco-facial-recognition-ban/index.html.

[238] Rachel Sandler, «San Francisco Bans Facial Recognition Technology», *Forbes*, 14 maggio 2019, https://www.forbes.com/sites/rachelsandler/2019/05/14/san-francisco-about-to-ban-facial-recognition/.

moratoria piuttosto che di un divieto assoluto, al fine di poter beneficiare in futuro degli eventuali sviluppi e miglioramenti. Inoltre, reputa fondamentale la previsione di alcune eccezioni a tali limitazioni, quali ad esempio l'impiego nei grandi eventi pubblici allo scopo di garantire la sicurezza della città. Ma non solo, anche Jonathan Turley, costituzionalista alla George Washington University, ha affermato che vietare in assoluto l'impiego di TRF significa negare il valore che questi strumenti hanno per la salvaguardia della sicurezza pubblica. Lo stesso è sostenuto anche dall'associazione degli ufficiali di polizia di San Francisco, che, pur consapevole che non si tratti di una tecnologia accurata al 100%, non manca di evidenziare le molteplici potenzialità che tali strumenti offrono nelle attività d'indagine.[239]

L'*Information Technology and Innovation Foundation* ha dichiarato che la scelta effettuata dalla città non sia un modello da seguire, in quanto alcuni usi risultano adeguati e alle volte fondamentali per garantire l'ordine cittadino: basti pensare all'impiego che può essere realizzato nella lotta al terrorismo.[240]

Seppur, come si può evidenziare dalla trattazione appena svolta, sono state molte le critiche che sono susseguite alla decisione della città di San Francisco, molte altre città degli USA hanno deciso di adottare delle ordinanze simili, volte a vietare lo strumento di identificazione biometrica impiegato dai dipartimenti di polizia.

Nel giugno 2019, seguendo l'esempio di San Francisco, la città di Somerville (Massachusetts) vieta l'impiego della tecnologia di riconoscimento facciale, quale strumento impiegato negli spazi pubblici, diventando così la seconda città negli USA ad aver posto un divieto generale per l'uso di tale sistema. L'ordinanza, approvata dal consiglio comunale però non ha trovato questa volta pieno appoggio da parte di ACLU of Massachusetts: secondo Kade Crockford, direttrice di *Technology for Liberty Program* (progetto che lavora affinché la nuova tecnologia rafforzi piuttosto che comprometta i diritti fondamentali), sarebbe stata più idonea la previsione di una

[239] Kate Conger, Richard Fausset, e Serge F. Kovaleski, «San Francisco Bans Facial Recognition Technology», *The New York Times*, 14 maggio 2019, par. U.S., https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html; Laura Hautala, «San Francisco Becomes First City to Bar Police from Using Facial Recognition», CNET, 14 maggio 2019, https://www.cnet.com/tech/services-and-software/san-francisco-becomes-first-city-to-bar-police-from-using-facial-recognition/.

[240] Shannon Van Sant e Richard Gonzales, «San Francisco Approves Ban On Government's Use Of Facial Recognition Technology», 14 maggio 2019, par. Technology, https://www.npr.org/2019/05/14/723193785/san-francisco-considers-ban-on-governments-use-of-facial-recognition-technology.

pausa nell'impiego della TRF, in modo da permettere al governo di poter predisporre una regolamentazione a livello statale, che disciplini la tecnologia in questione, limitandone gli usi e garantendo un controllo, ad esempio mediante la creazione di istituti *ad hoc*, cosa che risulta essere impossibile a livello locale.[241] La misura adottata ha trovato però forte sostegno popolare, alimentato dalla paura di essere sottoposti ad una sorveglianza constante e generale. Il suo sponsor principale, Ben Ewen-Campen, consigliere comunale della città di Somerville, ha dichiarato come tali risultati sono stati ottenuti a seguito di una diffusione degli strumenti senza trasparenza, linee guida, regolamenti della TRF e inoltre in totale assenza di una comprensione da parte della popolazione del loro funzionamento.[242]

Circa un mese dopo, sempre con il supporto di ACLU, anche la città di Oakland ha approvato all'unanimità un'ordinanza volta ad imporre un divieto dell'uso delle TRF negli spazi pubblici[243]. Tale disposizione emenda una legge del 2018, che prevede l'approvazione da parte del presidente della *Oakland's Privacy Advisory Commission*, ogni qual volta un membro del personale comunale "Seeking or soliciting funds for new surveillance technology".[244]

Il capo della polizia, Anne Kirkpatrick, in un report ha dichiarato come le forze dell'ordine non sono in possesso di tali strumenti e non ne fanno uso; tuttavia, secondo il capo della polizia essi possono risultare molto utili e per questo si schiera in modo contrario alla messa al bando della tecnologia.[245]

---

[241] Katie Lannan, «Somerville Bans Government Use Of Facial Recognition Tech», 28 giugno 2019, https://www.wbur.org/news/2019/06/28/somerville-bans-government-use-of-facial-recognition-tech; Caroline Haskins, «A Second U.S. City Has Banned Facial Recognition», *Vice* (blog), 28 giugno 2019, https://www.vice.com/en/article/paj4ek/somerville-becomes-the-second-us-city-to-ban-facial-recognition.

[242] Rachel Metz Business CNN, «Beyond San Francisco, more cities are saying no to facial recognition», CNN, consultato 19 febbraio 2022, https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html.

[243] «Ordinance No. 13635 | Code of Ordinances | Oakland, CA | Municode Library» (2019); Colin Lecher, «Oakland City Council Votes to Ban Government Use of Facial Recognition», The Verge, 17 luglio 2019, https://www.theverge.com/2019/7/17/20697821/oakland-facial-recogntiion-ban-vote-governement-california.

[244] «Chapter 9.64 - REGULATIONS ON CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY | Code of Ordinances | Oakland, CA | Municode Library» (2019).

[245] Sarah Ravani, «Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns», *San Francisco Chronicle*, 17 luglio 2019, par. Bay Area & State, https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php; Caroline Haskins, «Oakland Becomes Third U.S. City to Ban Facial

A seguito di tali decisioni assunte da molte città, altre han deciso di seguire tali esempi: nel Massachusetts, dopo la città di Somerville, si sono susseguite ordinanze volte a vietare l'uso del TRF da parte della polizia o di altri dipartimenti pubblici nelle città di Brookline, Cambridge, Northampton, Springfield, Boston, sempre al fine di evitare il perpetrarsi di discriminazioni causate da *bias* presenti in tali mezzi, che ricadono principalmente a danno della popolazione nera. Lo stato ha approvato una legge a fine 2020 volta a riformare l'organizzazione delle forze dell'ordine, che in un primo momento sembrava essere la più ampia legge approvata a livello statale volta ad imporre limiti stringenti all'uso di TRF da parte della polizia. Tuttavia, il disegno di legge, approvato da senato e camera, ha subito un indebolimento ad opera del Governatore Baker, il quale ha emendato il testo originario, onde evitare di imporre divieti nel lavoro perseguito per la sicurezza nel paese da parte degli agenti.[246] Non mancano comunque progetti e campagne volte alla modifica di tale legge, in vigore dal luglio 2021, al fine di condurre il paese ad imporre limitazioni uniformi per l'uso degli strumenti in uso della polizia molto invasivi, cosicché sia effettiva la tutela dei diritti della popolazione.[247]

Ma oltre a queste città, altre nei diversi stati hanno approvato atti normativi simili: si assiste ad ordinanze a Portland in Oregon, in California le città di Alameda, Berkeley, in Missisipi la città di Jackson, oltre che allo stato del Maine.

Seppur emblematici e degni di emulazione appaiono gli atti adottati da queste città, la maggior parte degli stati negli USA sembra essersi posta in una linea più moderata, volta a limitare, e non vietare, l'uso del riconoscimento facciale per conto delle forze dell'ordine.

Recognition», *Vice*, 17 luglio 2019, https://www.vice.com/en/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz; Anne E. Kirkpatrick, «Facial Recognition Ordinance Amendment - Supplemental Report» (Oakland: Chief of Police, 17 giugno 2019).

[246] Emma Peaslee, «Massachusetts Pioneers Rules For Police Use Of Facial Recognition Tech», *NPR*, 7 maggio 2021, par. Technology, https://www.npr.org/2021/05/07/982709480/massachusetts-pioneers-rules-for-police-use-of-facial-recognition-tech; Matt Murphy, «With Veto Threat, Baker Seeks Several Changes To Landmark Police Reform Bill», diembre 2020, https://www.wbur.org/news/2020/12/10/massachusetts-governor-proposed-amendments-policing-legislation; Charles Baker D., «Amendments on Police reform bill» (2020), https://d279m997dpfwgl.cloudfront.net/wp/2020/12/policing-amendment-letter.pdf.

[247] Jake Laperruque, «Testimony in Support of Massachusetts Legislation to Regulate Face Surveillance», Project On Government Oversight, 23 novembre 2021, https://www.pogo.org/testimony/2021/11/testimony-in-support-of-massachusetts-legislation-to-regulate-face-surveillance/.

Nel febbraio 2021 lo stato di Virginia ha adottato un'ordinanza molto stringente, che impone un divieto nell'acquisto e nell'impiego delle TRF a livello locale, salvo il caso in cui vi sia un'autorizzazione espressa dello stato. La regolamentazione ha trovato chiaramente l'opposizione del corpo di polizia, dove la *National Sheriff's Association* ha dichiarato, per mezzo del suo CEO e direttore Jonathan Thompson, come questo sia solo uno degli strumenti nelle mani della polizia; secondo quanto affermato è presente, inoltre, una disciplina che stabilisce i soggetti autorizzati ad utilizzare tali mezzi e ad accedere ai diversi database, con ciò non lasciando libero accesso a chiunque.[248]

Sebbene lo stato lo scorso anno abbia adottato tale ordinanza, i legislatori stanno promuovendo l'approvazione di un nuovo progetto di legge che permetta alla polizia l'utilizzo della TRF in casi specifici, ovvero al fine di risolvere un crimine o per garantire la sicurezza pubblica.[249]

Altri stati si sono cimentati in atti normativi che disciplinano tali strumenti, tra i quali lo stato di New York, il New Hampshire, il Texas, l'Oregon e l'Illinois.

Degno di menzione risulta essere il caso dell'Illinois, il quale nel 2008 ha approvato una legge, *Biometric Identification Privacy Act* (BIPA), che disciplina, nel settore privato, gli obblighi in capo ai soggetti che trattano dati biometrici, inclusi il rilevamento del volto di una persona, prevendendo l'informativa e il consenso del loro utilizzo. Ciò che risulta maggiormente innovativo consiste nella facoltà offerta ai soggetti interessati di citare in giudizio le società e i datori di lavori che usano in modo non lecito i propri dati biometrici: in virtù di ciò alcune grosse compagnie, quali Facebook, Google, sono stati citati in giudizi per aver scansionato e archiviato le loro foto dei volti senza il consenso degli utenti.[250] Seppur la BIPA rivolga una tutela per quanto attiene le aziende private, mediante un approccio individualista e procedurale alla privacy, ha dato prova ai legislatori di come sia indispensabile una regolamentazione della privacy biometrica anche negli spazi pubblici, offrendo perciò

[248] Julie Carr Smyth, «States Push Back against Use of Facial Recognition by Police», *AP NEWS*, 5 maggio 2021, par. Ohio, https://apnews.com/article/race-and-ethnicity-health-coronavirus-pandemic-business-technology-e4266250f7e2d691d4d664735c2c6bc0.

[249] Jonah Chester, «Virginia Bill Would Expand Police Use of Facial-Recognition Technology», Public News Service, 17 febbraio 2022, https://www.publicnewsservice.org/index.php?/content/article/77904-1.

[250] Rivera v. Google (2017); State of Illinois v. Facebook & Cambridge Analytica (2018).

una valida guida da seguire, in grado di delineare cosa manca nella legislazione vigente.[251]

In una posizione permissiva si è posto in un primo momento lo stato di Washington che nel 2020 ha approvato una legge, supportata dall'azienda Microsoft (che ha sede nella città), volta a consentire alla polizia un uso massivo della tecnologia. La legge prevedeva delle limitazioni al suo impiego, ma con una portata molto limitata sull'azione delle forze dell'ordine, alle quali sarebbe stato sufficiente fornire una dichiarazione di intenti prima del suo impiego e ottenere il consenso dell'interessato, salvo i casi di emergenza.[252] In opposizione alla legge si è posta fin da subito ACLU, impegnata da sempre nella lotta per i diritti civili, che in un comunicato stampa si è detta "extremely disappointed" per l'approvazione della legge, continuando così a non garantire adeguata protezione alle minoranze etniche.[253] Tuttavia la contea di King nello stato di Washington nel giugno 2021 ha adottato una decisione che stabilisce un divieto dell'utilizzo della tecnologia da parte di tutte le agenzie del governo locale, incluso lo sceriffo, salvo i casi in cui questa venga impiegata da organi federali per la ricerca di bambini scomparsi e nel caso di prove derivanti dall'uso riconoscimento facciale, ma non richiesto dai dipartimenti.[254]

Come è chiaramente dimostrato nella trattazione fin qui svolta, lo scenario legislativo che caratterizza gli Stati Uniti risulta essere ampiamente eterogeneo, con stati e città che si pongono in posizione completamente opposte. È auspicabile, perciò, un intervento del legislatore federale che vada a uniformare la posizione degli stati in

[251] Woodrow Hartzog, «BIPA: The Most Important Biometric Privacy Law in the US?», SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 30 ottobre 2020), https://papers.ssrn.com/abstract=3722053; Thomas Germain, «Why Illinois Has Become a Battleground for Facial Recognition Protection», Consumer Reports, 29 maggio 2020, https://www.consumerreports.org/privacy/why-illinois-has-become-a-battleground-for-facial-recognition-protection-a1376302521/.

[252] Andy Kingman, «In Washington State's landmark facial recognition law, public sector practices come under scrutiny and regulation | Insights | DLA Piper Global Law Firm», DLA Piper, 22 aprile 2020, https://www.dlapiper.com/en/us/insights/publications/2020/04/in-washington-states-landmark-facial-recognition-law-public-sector-practices-come-under-scrutiny/.

[253] «ACLU-WA Statement on Insufficient Facial Recognition Regulations (SB 6280) Becoming Law», American Civil Liberties Union, 31 marzo 2020, https://www.aclu.org/press-releases/aclu-wa-statement-insufficient-facial-recognition-regulations-sb-6280-becoming-law.

[254] Aya Elamroussi, «This Washington county is the first to ban facial recognition technology, official says», CNN, 2 giugno 2021, https://www.cnn.com/2021/06/02/us/facial-recognition-technology-ban/index.html.

merito a tale materia, al fine di garantire i diritti civili delle persone, ma che allo stesso tempo riesca a sfruttare le potenzialità che lo sviluppo tecnologico fornisce a ciascuno di noi quotidianamente, sia relativamente alla sicurezza, ma anche per quanto attiene il miglioramento della vita.

4.4 Il caso Clearview AI e gli altri produttori di software di riconoscimento facciale

Clearview AI è una società, ideata nel 2017 da Hoan Ton-That e Richard Schwartz, operante nel settore IT, che fornisce software di riconoscimento facciale, principalmente al fine di supportare l'attività delle forze dell'ordine e delle agenzie governative.[255]

Si tratta di un sistema di un riconoscimento facciale *ex post*, il cui funzionamento si basa sul *matching* di foto: caricata l'immagine che si intende identificare nella piattaforma, questa viene confrontata con quelle presenti nel database del programma, al fine di apprendere se vi sia corrispondenza di identità, con il risultato di identificare la persona in questione in caso di riscontro positivo. La caratteristica principale della piattaforma è costituita dal suo database, che contiene più di tre miliardi di foto di soggetti, prese dai numerosi siti internet e dai diversi social network, che allo stesso tempo può dirsi essere stata la causa che ha condotto la società al centro di un dibattito in merito alla violazione della privacy. Nel gennaio 2020 Kashmir Hill giornalista del New York Times, ha pubblicato un'inchiesta giornalistica che ha rivelato come la società abbia agito, fin dal momento in cui è stata creata, in modo segreto, senza che le persone fossero a conoscenza dell'uso di tale strumento da parte di molte autorità ma non solo, anche senza sapere che le proprie foto erano state inserite all'interno di un immenso archivio.[256] Solo a seguito della pubblicazione di tale indagine, si ha avuto piena consapevolezza di cosa la società stesse compiendo.

Clearview AI, raccogliendo e utilizzando le immagini e le informazioni presenti nel web e nei social network ha violato i termini di servizio di questi, accettati al

[255] «Clearview AI», in *Wikipedia*, 1 gennaio 2021, https://it.wikipedia.org/w/index.php?title=Clearview_AI&oldid=117680562.

[256] Kashmir Hill, «The Secretive Company That Might End Privacy as We Know It», *The New York Times*, 18 gennaio 2020, par. Technology, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

momento della loro iscrizione, che vietano espressamente l'uso dei dati personali condivisi nella piattaforma. Ton-Than ha affermato pubblicamente "So the way we have built our system is to only take publicly available information and index it that way" sulla base della convinzione che se un'informazione viene resa nota al pubblico del web, non può essere degna di protezione. Ma è proprio in virtù di tale dichiarazione, attestante il modo di agire del software, che la compagnia è stata oggetto di plurime azioni da parte di Twitter, Facebook, YouTube, LinkedIn e Venmo. Secondo quanto riporta a CBS News Alex Joseph, portavoce di YouTube, "YouTube's Terms of Service explicitly forbid collecting data that can be used to identify a person. Clearview has publicly admitted to doing exactly that, and in response we sent them a cease-and-desist letter". Sulla stessa linea si pongono anche le altre piattaforme, tra cui Twitter ha inoltre richiesto la cancellazione di tutti i dati presi dal sito, dichiarando in una nota resa pubblicamente come il valore principale del social network consiste proprio nella difesa e nel rispetto delle voci di ciascuno, preservando la privacy dei propri utenti.[257] Dunque, la posizione assunta dalla società, per quanto attiene la pubblicazione delle immagini prese dal web, risulta essere scorretta non solo in relazione al senso comune, ma anche per quanto attiene il rispetto della legge. Ciononostante, i legali dell'azienda intendono costruire la difesa su casi relativi all'era predigitale, per evidenziare come ci sia una riduzione della privacy nel momento in cui si è in pubblico: tra questi vi è la nota sentenza del 1975, *Cox Broadcasting Corp v. Cohn*[258], nella quale la corte della Georgia ha ritenuto che, laddove il nome di una vittima di stupro sia stato pubblicato in un verbale e poi divulgato, la capacità del governo di vietarne la successiva pubblicazione trova un limite nel Primo Emendamento[259], che garantisce appunto la libertà di espressione. Lo stesso principio è stato ribadito poi dalla sentenza *Florida Star v. B.J.F* della *United States Supreme Court*, sempre relativo alla divulgazione del nome di una vittima di stupro.

[257] Gisela Perez e Hilary Cook, «Clearview AI: Google, YouTube Venmo and LinkedIn send cease-and-desist letter to facial recognition app that helps law enforcement.», CBS News, 5 febbraio 2020, https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/.

[258] Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (Court of Georgia 3 marzo 1975).

[259] «Primo emendamento delle Costituzione degli Stati Uniti»: "*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances*".

L'obbiettivo nel prendere esempio da tali precedenti è quello di porre l'attenzione sul concetto "publicy accessible information", come se tale nozione permettesse loro di compiere qualsiasi azione. Ma le sentenze a cui i legali intendono riferirsi sono casi che trattano di questioni di interesse pubblico, come i procedimenti giudiziari; al contrario, come affermato in *Snyder v. Phelps*[260], la limitazione della parola su questioni private non implica preoccupazioni a livello costituzionale, non si tratta di una limitazione alla libertà di parola: è questo il caso delle informazioni raccolte da Clearview AI, dati estremamente personali e privati che vengono usati dalle autorità per sorvegliare le persone.[261] Appare perciò scorretto sostenere che il Primo Emendamento e la protezione della privacy siano in collisione tra loro, dove quest'ultima, secondo i grandi Big Tech, andrebbe a limitare i diritti protetti da tale norma di primaria importanza. Questa posizione è stata difesa anche da Floyd Adams, un importante avvocato statunitense, da sempre impegnato nella difesa del Primo Emendamento, secondo il quale nello scontro tra i due, prevale sempre la norma costituzionale.[262] Più pertinente invece sembra essere una visione in cui il Primo Emendamento e la privacy siano complementari l'uno all'altro (infatti quest'ultima trova fondamento legislativo proprio nel Primo Emendamento), volti entrambi a garantire quei diritti che garantiscono la Rule of law, fondamentale per una sana democrazia.

Dopo una prima valutazione in merito a coloro i quali potevano ottenere l'applicazione, in un'intervista su FoxBusiness, il suo CEO Ton-Than ha dichiarato che Clearview AI è rivolta alle sole autorità, al fine di implementare gli strumenti a loro disposizioni per combattere la criminalità e risolvere in modo più facile e veloce casi giudiziari, non trattandosi dunque di un sistema di sorveglianza generalizzato o di

[260] Snyder v. Phelps, 562 U.S. 443 (U.S. Supreme Court 2011).

[261] Margot E. Kaminski e Scott Skinner-Thompson, «Free Speech Isn't a Free Pass for Privacy Violations», *Slate*, 9 marzo 2020, https://slate.com/technology/2020/03/free-speech-privacy-clearview-ai-maine-isps.html.

[262] Kashmir Hill, «Facial Recognition Start-Up Mounts a First Amendment Defense», *The New York Times*, 11 agosto 2020, par. Technology, https://www.nytimes.com/2020/08/11/technology/clearview-floyd-abrams.html; Kashmir Hill, «What We Learned About Clearview AI and Its Secret 'Co-Founder'», *The New York Times*, 18 marzo 2021, par. Technology, https://www.nytimes.com/2021/03/18/technology/clearview-facial-recognition-ai.html.

un'applicazione ad uso privato.[263] I fondatori della piattaforma, al fine diffondere la tecnologia alle diverse autorità del paese, hanno offerto agli ufficiali di polizia periodi di prova gratuiti per 30 giorni, cosicché, una volta sperimentate le potenzialità, potessero incoraggiare i dipartimenti ad adottare tale rivoluzionario sistema. In questo modo si è assistito alla diffusione di un numero sempre maggiore di agenzie federali e governative che impiegavano tale tecnologia. Clearview AI ha distribuito il sistema a centinaia di dipartimenti di polizia, a FBI, *Customs and Border Protection* (CBP), Interpol e molti altri, comprendendo un utilizzo in ben 27 stati degli USA.[264]

Tuttavia, un'ulteriore indagine, svolta da BuzzFeed, una società di media e notizie statunitense, rivela come la piattaforma abbia provveduto a distribuire l'innovativo sistema a organizzazioni in tutto il mondo, permettendo dunque l'accesso costante a ciascuno, privo di un interesse meritevole, a un database ricco di identità di persone, che dovrebbe essere tutelato per il rispetto della privacy. Nella ricerca svoltasi è emerso come ripetutamente è accaduto che gli stessi enti fossero ignari del fatto che alcuni loro membri impiegavano nella loro attività il software di riconoscimento facciale, facendo emergere come il sistema non sia in grado di garantire l'accesso alle solo forze dell'ordine. Clare Garvey, membro del centro di Privacy e Tecnologia presso la *Georgetown Law*, ha dichiarato come, in merito alla mancanza di controllo e di regole chiare, "This is completely crazy ... There is not a clear line between law enforcement and non-law enforcement".[265]

La maggior parte dei clienti di Clearview AI sono dunque dipartimenti di polizia locale e statali; basti pensare al caso della polizia di Chicago che ha stipulato nel gennaio 2020 un contratto di due anni con Clearview AI.[266] La polizia di Chicago era già in possesso di un programma per il riconoscimento facciale dal 2013,

[263] «New Facial Recognition Tech "loved" by Law Enforcement: Clearview AI CEO», *Fox Business*, 19 febbraio 2020, http://video.foxbusiness.com/v/6133890195001/.

[264] Hill, «The Secretive Company That Might End Privacy as We Know It».

[265] Ryan Mac, Caroline Haskins, e Logan McDonald, «Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA», BuzzFeed News, 27 febbraio 2020, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[266] Tom Schuba, «CPD Using Controversial Facial Recognition Program That Scans Billions of Photos from Facebook, Other Sites», Chicago Sun-Times, 29 gennaio 2020, https://chicago.suntimes.com/crime/2020/1/29/21080729/clearview-ai-facial-recognition-chicago-police-cpd.

DataWorks[267], che utilizza un database interno di foto segnaletiche scattate nella città e nei dintorni; nonostante la presenza già di una tecnologia di identificazione biometrica, ha deciso di adottare anche il nuovo software in quanto contenente un database molto più ricco. ACLU of Illinois ha intentato causa contro la società di Ton-That per violazione dell'*Illinois Biometric Information Privacy Act*, legge che protegge gli abitanti dell'Illinois dalla raccolta di informazioni biometriche ad opera di aziende senza il proprio consenso. L'accusa rivolta alla società è quella di raccogliere dati personali senza l'assenso dei soggetti, di cercare e raccogliere immagini senza una causa probabile e negare alle persone il diritto a un giusto processo violando i termini dei siti Web. Il 27 agosto 2021 la corte dell'Illinois ha disposto a favore dell'associazione no-profit in merito alla causa, rigettando la mozione presentata da Clearview AI, volta a sostenere che l'attività della società sia protetta dal Primo Emendamento: una sua accettazione avrebbe invece comportato molto probabilmente la fine della libera espressione e di molte protezioni della privacy negli Stati Uniti.[268] L'obbiettivo della società, con tale richiesta, si può rinvenire nella distruzione della BIPA, che attualmente risulta essere la legge più importante sull'identificazione biometrica nel settore privato, in quanto permette all'interessato di citare direttamente in giudizio la società, che si suppone aver violato i propri diritti.[269] Tuttavia, ad oggi, la causa deve ancora essere portata al suo termine, per cui si dovrà attendere la decisione della corte per comprendere le sorti dell'uso di tale tecnologia altamente invasiva.

L'indagine svolta da BuzzFeed ha rivelato inoltre come tra l'elenco dei clienti del software ci siano anche diversi istituti scolastici, per un totale di circa 50 istituzioni educative in 24 stati. Ma non solo, in quanto sono numerosissime le aziende private, tra cui banche, supermercati, negozi, agenzie di sicurezza privata, che hanno stipulato un contratto formale con la società, e, seppur il software è stato utilizzato in un

[267] «Chicago Police Department: Face Recognition - Atlas of Surveillance», Atlas of surveillance, consultato 23 febbraio 2022, https://atlasofsurveillance.org/a/aos0978-chicago-police-department-face-recognition.

[268] ACLU v. Clearview AI (Corte dell'Illinois 28 maggio 2020); «Illinois Court Rejects Clearview's Attempt to Halt Lawsuit Against Privacy-Destroying Surveillance», American Civil Liberties Union, consultato 23 febbraio 2022, https://www.aclu.org/press-releases/illinois-court-rejects-clearviews-attempt-halt-lawsuit-against-privacy-destroying.

[269] Woodrow Hartzog, Neil Richards, e 2020, «Getting the First Amendment Wrong - The Boston Globe», *BostonGlobe.Com*, 4 settembre 2020, https://www.bostonglobe.com/2020/09/04/opinion/getting-first-amendment-wrong/.

periodo di prova gratuito, senza il rinnovo, ciò ha permesso ad un numero vastissimo di utenti privati di accedere al database, andando a ottenere informazioni altamente private, con il rischio molto elevato di un abuso.[270]

Ancor più preoccupante però è la diffusione della piattaforma non limitatamente alla regione degli USA, ma anche a clienti internazionali, tra cui purtroppo vi sono paesi con regimi autoritari, che violano costantemente i diritti umani. Nonostante il suo CEO Hoan Ton-That abbia dichiarato che il software non sarebbe stato diffuso in paesi contrari all'ideologia statunitense e non rispettosi della Rule of Law,[271] un documento ottenuto tramite una richiesta di registri pubblici rivela come la società abbia dichiarato l'intenzione di espandersi in altri 22 paesi, tra i quali emergono Arabia Saudita, Emirati Arabi, Qatar e Singapore, i cui codici penali considerano l'omosessualità come un crimine.[272] Perciò l'uso della tecnologia in questione in paesi con regimi autoritari potrebbe avere delle conseguenze molto importanti nei confronti della popolazione, incidendo sulla privacy, sulla libertà di movimento ed espressione delle persone, al punto tale da mettere in pericolo la vita di coloro i quali sono considerati ostacolo alla comunità, quali attivisti politici, giornalisti, dissidenti politici, ma anche di quelle persone più vulnerabili, come la comunità LGBTQ, donne e bambini.

La piattaforma si è diffusa presto anche in Europa, dove, a seguito di alcuni primi utilizzi da parte di determinati stati, si è assistito a partire dal 2020 all'apertura di indagini avviate dalle autorità di regolamentazione dei diversi paesi, volte a verificare se il software viola le norme in tema di privacy. Nel giugno del 2020 si è espresso in merito anche l'European Data Protection Board, il quale emesso una guida secondo la quale Clearview AI non sembra rispettare le norme del GDPR.

Un ulteriore pericolo in cui una tale piattaforma può incorrere è la violazione di dati ad opera di attacchi informatici, cosa che, per un programma basato sulla raccolta

[270] Mac, Haskins, e McDonald, «Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA».

[271] «Clearview AI CEO Defends Facial Recognition Software», *Amanpour & Company*, 19 febbraio 2020, https://www.pbs.org/wnet/amanpour-and-company/video/clearview-ai-ceo-defends-facial-recognition-software/.

[272] Caroline Haskins McDonald Ryan Mac, Logan, «Clearview AI Wants To Sell Its Facial Recognition Software To Authoritarian Regimes Around The World», BuzzFeed News, 6 febbraio 2020, https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22.

di informazioni, può causare molti più danni di quanti se ne possono generare in altri software. L'accesso non autorizzato ai server di Clearview AI permette la presa visione di tutti i dati che compongono l'enorme database, in cui rientra ciascun soggetto che ha pubblicato delle foto in qualche piattaforma o nel web, e l'elenco dei clienti della società. Ciò è quanto è accaduto: la società ha inviato una notifica ai propri clienti dichiarando come fosse avvenuto un accesso non autorizzato, ma che non era stato in grado di violare alcun dato. Un legale della società, Tor Ekeland, ha riferito in una dichiarazione al The Daily Best "Security is Clearview's top priority. Unfortunately, data breaches are part of life in the 21st century. Our servers were never accessed. We patched the flaw and continue to work to strengthen our security".[273]

A seguito delle inchieste condotte dal New York Times e da BuzzFeed e dalle cause legali intraprese in tutto il paese contro Clearview AI, in merito alle attività svolte in assenza di trasparenza e in violazione delle normative vigenti, la società ha dichiarato "Clearview is cancelling the accounts of every customer who was not either associated with law enforcement or some other federal, state, or local government department, office, or agency".[274]

Il software è stato impiegato anche per individuare le persone responsabili dell'attacco del 6 gennaio 2021 a Capitol Hill: le forze dell'ordine hanno dichiarato di aver usato il programma, attingendo le immagini dai social e dai diversi video pubblicati. L'uso della tecnologia da parte delle forze dell'ordine è aumentato del 26% a seguito di tali eventi, proprio in concomitanza con le ricerche dei responsabili dell'aggressione al Campidoglio degli estremisti di destra. Ma chiaramente tale modalità di agire appare allarmante per la democrazia americana.[275]

[273] Betsy Swan, «Facial-Recognition Company That Works With Law Enforcement Says Entire Client List Was Stolen», *The Daily Beast*, 26 febbraio 2020, par. tech, https://www.thedailybeast.com/clearview-ai-facial-recognition-company-that-works-with-law-enforcement-says-entire-client-list-was-stolen.

[274] Ryan Mac, Caroline Haskins, e Logan McDonald, «Clearview AI Says It Will No Longer Provide Facial Recognition To Private Companies», BuzzFeed News, 8 maggio 2021, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies.

[275] Joan Donovan e Chris Gilliard, «Facial Recognition Technology Isn't Good Just Because It's Used to Arrest Neo-Nazis», *Slate*, 12 gennaio 2021, https://slate.com/technology/2021/01/facial-recognition-technology-capitol-siege.html.

Tuttavia il 31 gennaio 2022 la società ha dichiarato, in un comunicato stampa, di aver ottenuto il brevetto statunitense "Methods for Providing Information About a Person Based on Facial Recognition", per la capacità unica di riconoscimento facciale della sua piattaforma, che secondo la National Institute of Standards & Technology (NIST) Test funziona in modo quasi impeccabile.[276] La notizia era già trapelata a fine dicembre 2021, dove il giornale il Politico aveva riportato l'informazione.[277] Ciò ha permesso dunque all'azienda con il database di più vasto in assoluto, contenente più di 10 miliardi di foto, una protezione della proprietà intellettuale, distinguendosi così dalle altre aziende che si erano cimentate nella creazione di software di riconoscimento facciale.

Tra le altre aziende che si sono affacciate nel mondo statunitense del commercio di software di riconoscimento facciale vi sono, oltre alla società di Ton-That, anche IBM, Microsoft e Amazon.

L'International Business Machine Corporation (IBM) è un'azienda operante nel settore informatico, che si annovera tra i più grandi e longevi Big Tech. Anch'essa ha sperimentato la creazione di software di riconoscimento facciale, ma nel giugno 2020 ha deciso di interrompere la sperimentazione, a seguito delle inchieste svolte sul suo competitor, Clearview AI, che hanno portato alla luce come tali sistemi risultino altamente invasivi della privacy e degli studi svolti dalla MIT in merito alla presenza di *bias* nei software, che conducono a discriminazioni nei confronti della popolazione nera. La notizia è giunta mediante un comunicato stampa, a cui ha fatto seguito una lettera al Congresso, nella quale il suo CEO Arvind Krishna ha condannato tali software per il loro potenziale utilizzo da parte della polizia volto a violare diritti umani e libertà fondamentali. Si tratta di una decisione presa al termine di un percorso di due anni, in cui si sono sperimentate le difficoltà, le imprecisioni e il rischio per una sorveglianza di massa. IBM, si legge nella lettera, offre inoltre al Congresso il suo aiuto nel creare un sistema che possa perseguire la giustizia e l'equità razziale.[278]

[276] «Clearview AI's Revolutionary Facial Recognition Platform Awarded U.S. Patent», Clearview AI, 31 gennaio 2022, https://www.clearview.ai/press-release-clearview-ais-revolutionary-facial-recognition-platform-awarded-us-patent.

[277] Alessandra S. Levine, «Clearview AI on Track to Win U.S. Patent for Facial Recognition Technology», *POLITICO*, 4 dicembre 2021, https://www.politico.com/news/2021/12/04/clearview-ai-facial-recognition-523735.

[278] «IBM's Decision to Abandon Facial Recognition Technology Fueled by Years of Debate», *Washington Post*, consultato 24 febbraio 2022,

Tuttavia, secondo l'associazione *Privacy International*, le parole usate dal CEO sarebbero vaghe, tanto che l'uso di "scopi generali" indicherebbe che la società non avrebbe abbandonato la vendita della tecnologia in questione nel caso di prodotti personalizzati. A ciò si aggiunge che la società fino ad allora aveva venduto tali software a numerosi dipartimenti di polizia, utilizzando il termine "smart cities", ad indicare l'obbiettivo di creare città dove sorveglianza e sicurezza erano alla base della vita sociale.[279]

A seguito di ciò anche Amazon, che ha realizzato nel 2016 il software di riconoscimento facciale Amazon Rekognition, ha dichiarato il 10 giugno di adottare una moratoria di un anno per l'uso del programma da parte della polizia, con la speranza che il governo emani delle norme più severe per l'uso etico della tecnologia. Tuttavia, la società ha deciso di continuare a garantirne l'uso a organizzazioni volte a salvare le vittime della tratta di esseri umani e riunire i bambini scomparsi con le loro famiglie.[280] In assenza di qualunque decisione da parte del governo federale e a seguito dell'escalation delle proteste contro la brutalità della polizia, il 18 maggio 2021 la stessa azienda ha prolungato la sospensione fino a nuovo avviso.[281]

L'11 giugno 2020 l'altra grande Big Tech, Microsoft, ha dichiarato, in concordanza con le azioni intraprese da IBM e Amazon Rekognition, di sospendere la vendita di software di riconoscimento facciale alla polizia fintantoché il governo federale non provvederà con regole chiare in merito all'uso della tecnologia.[282]

---

https://www.washingtonpost.com/technology/2020/06/11/ibm-facial-recognition/; Arvind Krishna, «IBM - Lettera al Congresso», 8 giugno 2020; «IBM Abandons "biased" Facial Recognition Tech», *BBC News*, 9 giugno 2020, par. Technology, https://www.bbc.com/news/technology-52978191.

[279] «IBM (Not) Ending Facial Recognition - Our Quick Thoughts», Privacy International, 11 giugno 2020, http://privacyinternational.org/news-analysis/3898/ibm-not-ending-facial-recognition-our-quick-thoughts.

[280] Amazon staff, «We Are Implementing a One-Year Moratorium on Police Use of Rekognition», Amazon, 10 giugno 2020, https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition.

[281] Jeffrey Dastin, «Amazon Extends Moratorium on Police Use of Facial Recognition Software», *Reuters*, 18 maggio 2021, par. Technology, https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/.

[282] Jay Greene, «Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM», *Washington Post*, 11 giugno 2020, https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.

4.5 Attuali utilizzi delle TRF da parte di organi pubblici

La diffusione dei sistemi di riconoscimento facciale ha interessato nell'ultimo decennio molti organi pubblici degli USA, impegnati costantemente nel garantire la sicurezza del paese (in modo particolare per evitare attacchi terroristici) e nel risolvere investigazioni criminali.

L'introduzione di tale tecnologia in apparati federali o statali ha suscitato molto interesse da parte di numerosi studiosi, che si sono cimentati ben presto in ricerche volte a delineare con che ampiezza lo strumento in questione è stato adottato nel settore pubblico, vista l'assenza di norme che disciplinassero se e in che modo le TRF potessero essere date in dotazione ai diversi agenti.

Tra i più importanti studi svolti si rinviene quello pubblicato nel 2016 dal Center on Privacy & Technology della Georgetown Law, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, che attestava come, già 6 anni fa, 117 milioni di americani fossero sottoposti a sistemi di riconoscimento facciale e non ci fosse la presenza di un quadro regolatorio che disciplinasse il modo in cui impiegare tali sistemi. L'obbiettivo perseguito dal report si rinviene nell'evidenziare come tali sistemi possano comportare effetti negativi sulla privacy delle persone, riducendo diritti civili e libertà. L'analisi in questione prende a riferimento l'FBI e più

di 100 agenzie, statali e locali, alle quali sono stati inviate richieste del *Freedom of Information Act* e interviste, da cui emerge che ben 52 agenzie, tra cui l'FBI, nel momento in cui è stata svolta la ricerca, usavano o han usato la TRF. Ciò che si può dedurre dallo studio perseguito è che più di un quarto di tutte le forze dell'ordine statali e locali americane eseguivano ricerche di riconoscimento facciale nei propri database, in quelli di altre agenzie o avevano la possibilità di accedere ai loro sistemi. Per quanto attiene ad una sua regolamentazione, il team è riuscito ad individuare uno standard legale solo per 24 della totalità delle agenzie prese in considerazione: tre richiedevano una causa probabile e 10 richiedevano un ragionevole sospetto; le altre 11 invece richiedevano uno scopo di giustizia o non fornivano documentazioni che indicassero uno standard legale. Perciò solo 13 agenzie ponevano come requisito per accedere al sistema di identificazione biometrica un qualsiasi grado di sospetto individualizzato (ragionevole o causa probabile).[283]

Un ulteriore studio, *The Facial Recognition World's Map - Smile You're on Camera*, condotto da Surfshark ha preso in analisi la diffusione a livello globale della TRF. L'analisi svolta rileva come negli USA circa 24 aeroporti hanno adottato tali sistemi, mentre ben 30 dipartimenti di polizia locale e statale impiegano la tecnologia di identificazione biometrica nelle loro attività.[284]

Inoltre, un rapporto del Washington Post del 2019 ha rivelato come il governo federale abbia creato un enorme database di riconoscimento facciale contenente tutte le foto delle patenti dei conducenti in USA.[285]

Tuttavia, non solo enti privati han condotto inchieste, in quanto anche il *Governament Accountability Office* (GAO), una sezione investigativa del Congresso degli Stati Uniti, con competenza in diverse materie, ha condotto diverse ricerche in merito all'impiego di tali strumenti. Nell'estate 2021 ha pubblicato due report che delineano l'utilizzo della tecnologia di identificazione biometrica per conto delle agenzie e dipartimenti federali.

[283] Garvie, Bedoya, e Frankle, «The Perpetual Line-Up».

[284] «The Facial Recognition World Map - Smile You're on Camera».

[285] Drew Harwell, «FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches», *Washington Post*, 7 luglio 2019, https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

Il primo studio, pubblicato nel giugno 2021, prende in analisi 42 agenzie federali, riportando, in un periodo di tempo che intercorre dal 2015 al 2020, quali forze dell'ordine federali impiegano la tecnologia di riconoscimento facciale nella propria mansione, in quali attività vengono usate e il modo in cui controllano l'uso di TRF di proprietà non federale in uso presso altri enti statali, locali o non governativi. Si tratta in verità di un report già pubblicato nell'aprile 2021, ma che a seguito di alcuni reclami da parte di alcuni dei dipartimenti descritti ha dovuto procedere alla creazione di una versione pubblica che ometta delle informazioni considerate sensibili.

La ragione che ha condotto ad analizzare 42 delle 86 agenzie federali analizzate nel 2016, in un altro report del GAO, è dipesa dal fatto che, secondo il *Council of the Inspectors General on Integrity and Efficiency*, nessun ufficio degli ispettori impiega tali strumenti: in virtù di ciò queste agenzie sono state escluse dall'analisi, ad accezione però della *Transportation Security Administration* che impiega agenti federali, ma che non era stata inserita nel report del 2016.[286]

Gli uffici federali hanno la possibilità di usare un sistema di loro proprietà, sistemi propri di agenzie governative e non, quali per esempio il già noto e discusso software Clearview AI, ma anche tecnologie in via di sviluppo/sperimentali. Nell'impiego di sistemi di entità private, i diversi dipartimenti hanno l'obbligo di rispettare il Privacy Act del 1974[287] che pone dei limiti alla raccolta, alla divulgazione e all'uso di dati personali da parte delle forze dell'ordine. Tale legge, letta in stretta relazione con la circolare A-130[288], garantisce che anche le tecnologie gestite da appaltatori esterni rispettino gli standard minimi per la tutela della privacy, così come disciplinato a livello federale.

[286] «Appendix I: Objectives, Scope, and Methodology - Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks» (United States Government Accountability Office, giugno 2021) p.34.

[287] «Privacy Act - An Act to amend title 5, United States Code, by adding a section 552a, to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes» (1974).

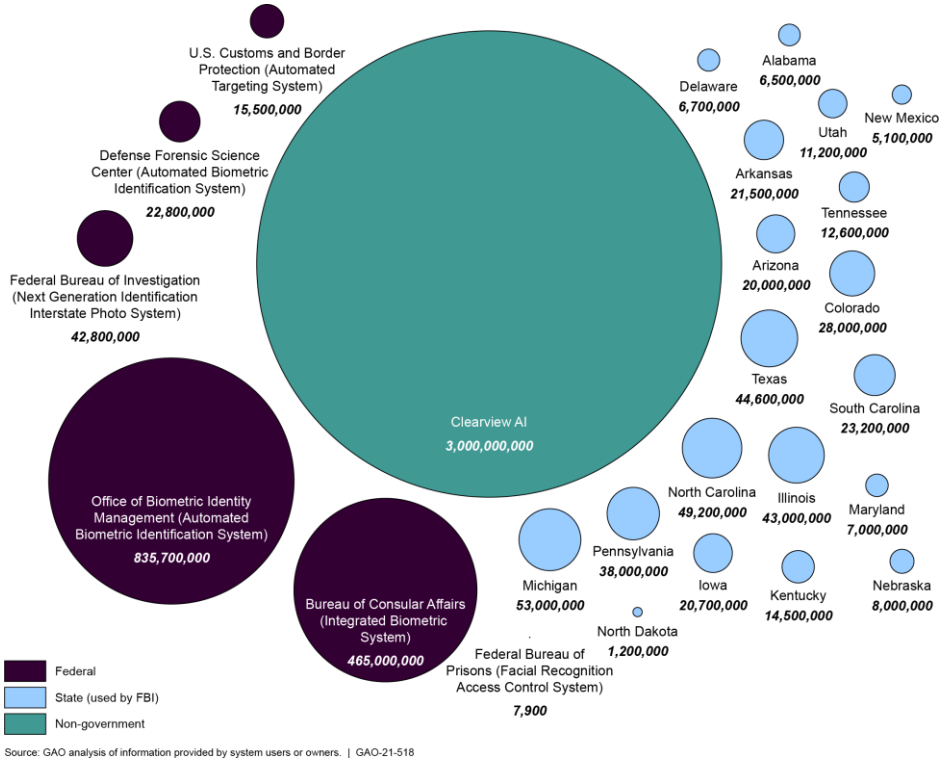
[288] «Circular no. A-130 - Managing Information as a Strategic Resource» (2016).

Il documento riporta come sulle agenzie intervistate, 20 abbiano impiegato nelle proprie attività il software di riconoscimento facciale, per un totale di 120000 agenti con accesso alle piattaforme. Di queste 20 agenzie, 3 sono in possesso di un solo sistema, 12 hanno impiegato la tecnologia di un'altra entità e 5 sono in possesso di un loro sistema ma ne impiegano anche un altro.

Source: GAO analysis of survey data. | GAO-21-518

Inoltre, si può constatare, analizzando il report, come delle 42 agenzie prese in esame, 17 di queste hanno impiegato software di altre entità: 15 hanno dichiarato di aver usato sistemi di entità federali, 14 han utilizzato sistemi di proprietà di enti statali, locali o territoriali e 11 han impiegato strumenti non governativi. Come risulta dal grafico sotto riportato, si può facilmente notare come la tecnologia commerciale (intendendosi sistemi non federali e non governativi) maggiormente impiegata dai diversi uffici federali sia Clearview AI, con ciò confermando le potenzialità di tale sistema altamente invasivo, che permette l'accesso al database più vasto tra quelli creati dai diversi software.[289]

[289] «FACIAL RECOGNITION TECHNOLOGY - Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks» (United States Government Accountability Office, giugno 2021) p.12.



Gli utilizzi principali di tali tecnologie hanno interessato soprattutto indagini criminali, ma non solo, in quanto sono state impiegate anche per la sorveglianza, la verifica dei viaggiatori, la ricerca e l'istruzione. Lo studio riporta che quattordici agenzie, delle venti che hanno affermato di usare nelle loro attività la TRF, han dichiarato di impiegare tali strumenti per svolgere indagini criminali. A seguito della morte di George Floyd, sei agenzie hanno rivelato di aver utilizzato la tecnologia per indagini penali relative a disordini civili, rivolte e proteste, volte ad individuare però soggetti sospetti.[290] Inoltre, tali sistemi sono stati ampiamenti usati da tre agenzie per le indagini sulle proteste di Capitol Hill verificatesi il 6 gennaio 2020[291]: la U.S. Capitol Police ha usato Clearview AI per la creazione di piste investigative; il Customs and Border Protection (CBP) ha usato il suo Automated Targeting System

[290] Maya Shwayder, «Police Facial Recognition Tech Could Misidentify Protesters», Digital Trends, 2 giugno 2020, https://www.digitaltrends.com/news/police-protests-facial-recognition-misidentification/.

[291] Kashmir Hill, «The Facial-Recognition App Clearview Sees a Spike in Use after Capitol Attack», *The New York Times*, 9 gennaio 2021, par. Technology, https://www.nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html.

per condurre ricerche su richiesta di un'altra agenzia federale; e infine il Bureau of Diplomatic Security ha usato il sistema biometrico integrato del Dipartimento di Stato per condurre ricerche su richiesta di un'altra agenzia federale.[292]

Nonostante si riscontri un maggior utilizzo nel campo delle indagini criminali, si può constatare come le attività appaiano le più varie: sorveglianza, controllo dell'identità (che a seguito della diffusione del Coronavirus-19 è diventata più difficile da eseguire da vicino), verifica del viaggiatore, accesso in determinate aree, ricerca e istruzione.[293]

Il report dimostra inoltre come, sulle 14 agenzie che han dichiarato di usare sistemi commerciali, 13 di queste non siano in grado di monitorare i propri dipendenti che impiegano tali sistemi e inoltre non sono neppure a conoscenza di quali sistemi siano impiegati.[294]

Con ciò sarebbe invece auspicabile un controllo interno dell'uso che viene fatto delle TRF, volto a evitare possibili abusi che possono essere compiuti o impieghi per utilizzi non strettamente necessari, volti semplicemente a creare un sistema di sorveglianza generalizzata. Il fatto di essere ignare di ciò che i loro dipendenti utilizzano, rende le agenzie non in grado di valutare i reali rischi che l'uso di tali strumenti comporta.

I requisiti di legge prevedono che nell'impiego di nuove tecnologie le agenzie debbano compiere una valutazione in merito al livello di invasione nella privacy che tale innovazione comporta: in mancanza di ciò si incorre nel rischio che i proprietari di tali sistemi condividano delle informazioni sensibili oppure che si verifichino violazioni in merito al set di dati, o ancora quelli legati all'accuratezza del sistema. Solamente l'U.S. Immigration and Customs Enforcement ha predisposto un *Privacy Impact Assessment for the ICE Use of Facial Recognition Services*, volto a

[292] «FACIAL RECOGNITION TECHNOLOGY - Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks» p.17-18.

[293] «FACIAL RECOGNITION TECHNOLOGY - Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks» p.19.

[294] «FACIAL RECOGNITION TECHNOLOGY - Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks» p.20-21.

predisporre una valutazione dei rischi connessi all'uso della tecnologia in questione e le eventuali azioni da intraprendere per ridurre tali rischi.[295]

Lo studio nella sua parte finale delinea una serie di raccomandazioni che invitano i diversi dipartimenti a tracciare quali sistemi non federali vengono impiegati dai diversi dipartimenti, predisponendo valutazioni di impatto dei rischi connessi con il loro utilizzo, inclusi quelli relativi alla privacy e all'accuratezza dello strumento.

Il secondo report, pubblicato nell'agosto 2021, invece esamina, su richiesta del Congresso, come le agenzie federali hanno usato TRF nell'anno fiscale 2020, comprendendo le interazioni con entità non federali, e il programma di espansione fino al 2023, allo scopo di sviluppare una comprensione completa dell'uso di tale innovativo strumento. Lo studio, nelle sue prime pagine, descrive cosa debba intendersi, secondo il Governament Accountability Office, per riconoscimento facciale: si riferisce non solo ad una tecnologia volta a rilevare se un volto corrisponde a quello di un soggetto la cui foto è già presente in un database, ma anche quelle tecnologie di analisi facciale (volte a categorizzare in base a sesso, età, ecc.) e di rilevamento facciale, per determinare se un volto è presente in una foto o video.[296]

La richiesta di tale analisi è stata presentata dai membri della Commissione giudiziaria della Camera e della Commissione per la supervisione e la riforma della Camera a seguito della diffusione di crescenti preoccupazioni sull'uso improprio della tecnologia di riconoscimento facciale.

Il report prende in esame 24 agenzie del *Chief Financial Officers Act* del 1990[297]: si tratta dei dipartimenti dell'agricoltura, del commercio, della difesa, dell'istruzione, dell'energia, della salute e dei servizi umani, della sicurezza interna, dell'alloggio e dello sviluppo urbano, dell'interno, della giustizia, del lavoro, dello stato, dei trasporti, del tesoro, degli affari dei veterani, dell'agenzia di protezione ambientale, dell'amministrazione nazionale aeronautica e spaziale, dell'agenzia americana per lo sviluppo internazionale, dell'amministrazione dei servizi generali, della fondazione nazionale della scienza, della commissione regolatrice nucleare, dell'ufficio di

[295] «Privacy Impact Assessment for the ICE Use of Facial Recognition Services DHS/ICE/PIA-054» (Homeland Security Investigation, 13 maggio 2020).

[296] «FACIAL RECOGNITION TECHNOLOGY - Current and Planned Uses by Federal Agencies» (United States Government Accountability Office, agosto 2021) p.5-6.

[297] «Chief Financial Officers Act» (1990).

gestione del personale, dell'amministrazione delle piccole imprese e dell'amministrazione della sicurezza sociale. A queste agenzie è stato sottoposto un questionario, al fine di raccogliere delle informazioni in merito a: i sistemi di TRF impiegati (di proprietà o a cui si accede) nell'anno fiscale 2020; i sistemi TRF che le agenzie hanno pianificato di utilizzare fino all'anno fiscale 2023; le attività di ricerca e sviluppo legate a tali strumenti delle agenzie; le transazioni finanziarie, o di altro tipo, che le agenzie hanno stipulato per l'uso della tecnologia in questione da parte di entità non statali; la misura in cui le agenzie hanno regolato l'uso di sistemi di identificazione biometrica da parte di entità non statali.[298]

Il report del GAO riporta come sulle 24 agenzie 18 abbiano dichiarato di aver usato la tecnologia per diversi scopi nell'anno preso a riferimento; 10 invece dichiarano di voler espandere il proprio sistema fino al 2023.[299]

Gli impieghi analizzati ripropongono sia quelli più banali dello sblocco del proprio smartphone che quelli più controversi, quali la ricerca di sospetti criminali. Si evince dal report, dunque, l'impiego della tecnologia per sette scopi diversi:

1. Accesso digitale e sicurezza informatica al fine di controllare l'uso di personal computer, smartphone e dispositivi digitali;
2. Applicazione della legge nazionale per identificare una pista o un persona di interesse in un'indagine, un soggetto scomparso o una vittima di crimine;
3. Sicurezza fisica per controllare e sorvegliare l'accesso a edifici o luoghi;
4. Sicurezza delle frontiere e dei trasporti, volti ad identificare viaggiatori che intendono entrare negli USA;
5. Sicurezza nazionale e difesa: le TRF vengono impiegate nell'identificazione di terroristi o in quella di cittadini stranieri per motivi di sicurezza nazionale;
6. Valutazione medica per confermare l'identità di un paziente;
7. Altro: qualsiasi uso che non rientri in quelli delineati.[300]

[298] «FACIAL RECOGNITION TECHNOLOGY - Current and Planned Uses by Federal Agencies» p. 3.

[299] «FACIAL RECOGNITION TECHNOLOGY - Current and Planned Uses by Federal Agencies» p.10 e p.26.

[300] «FACIAL RECOGNITION TECHNOLOGY - Current and Planned Uses by Federal Agencies» p. 7.

Degli obbiettivi pocanzi proposti si può appurare come i sistemi di identificazione biometrica vengono principalmente impiegati per controllare l'accesso digitale, per l'applicazione della legge nazionale e per garantire la sicurezza fisica.

L'appendice II[301] riporta specificatamente per ogni agenzia l'uso della tecnologia. Si può constatare dunque come il Dipartimento dell'Istruzione, il Dipartimento di Housing and Urban Development, la Nuclear Regulatory Commission e la Small Business Administration, secondo quanto riferito nei questionari inviati a ciascuno dal GAO, non hanno impiegato sistemi di TRF nell'anno fiscale 2020 e predisposto alcun piano per avere attività di TRF fino all'anno fiscale 2023. Il Dipartimento del lavoro, l'Agenzia degli Stati Uniti per lo sviluppo internazionale, l'Agenzia per la protezione dell'ambiente e l'Ufficio di gestione del personale hanno riferito di utilizzare il riconoscimento facciale solamente per sbloccare smartphone o tablet. La maggior parte degli altri dipartimenti invece hanno dichiarato sia di utilizzare TRF generalmente mediante sistemi di proprietà, accessi ai sistemi governativi, locali o commerciali di TRF (come Clearview AI) durante l'anno fiscale 2020 che di aver pianificato sistemi di TRF fino all'anno fiscale 2023.[302]

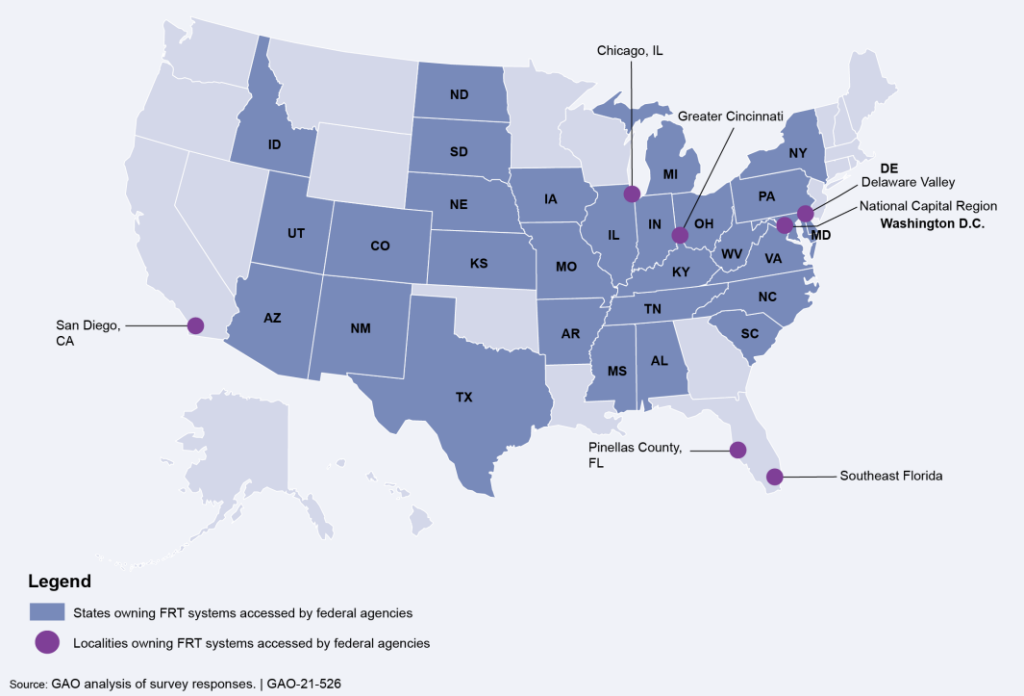
In modo particolare si può notare come 16 agenzie abbiano dichiarato di usare la tecnologia per l'accesso digitate o sicurezza informatica; 6 agenzie hanno usato tali strumenti per l'applicazione della legge nazionale; 5 agenzie impiegano TRF per la garantire la sicurezza pubblica; 2 dipartimenti per la sicurezza delle frontiere e de trasporti; 4 agenzie la usano per garantire la sicurezza nazionale e la difesa; infine 3 agenzie la usano per altri scopi, quali scopi, tra cui verificare l'identità degli individui che ricevono carte d'identità e badge temporanei.

Il report riferisce come 18 agenzie possiedono o accedono a sistemi di altre società: 17 possiedono o accedono a sistemi federali, 3 accedono a sistemi propri di enti statali (di proprietà di 29 statu e 7 località) e 6 accedono a sistemi di proprietà di fornitori commerciali.[303]

[301] «Appendix II: Summaries of Selected Federal Agencies' Facial Recognition Technology Activities - GAO-21-526 Facial Recognition Technology» (United States Government Accountability Office, agosto 2021).

[302] «Appendix II: Summaries of Selected Federal Agencies' Facial Recognition Technology Activities - GAO-21-526 Facial Recognition Technology».

[303] «FACIAL RECOGNITION TECHNOLOGY - Current and Planned Uses by Federal Agencies» pp. 12-20.



Gli studi fin qui analizzati mettono in luce le molteplici problematicità che l'impiego di tale tecnologia sta facendo emergere nella vita quotidiana di ciascuno di noi. Il fatto che tali strumenti siano stati impiegati a seguito delle proteste Black Lives Matter del 2015 a Oakland e Baltimora[304] e dopo la morte di George Floyd, come han dichiarato alcune agenzie prese in analisi da GAO, hanno degli effetti allarmanti, perché vengono impiegati dalle forze dell'ordine per reprimere il dissenso, cosa che in un paese democratico non può essere ammesso.

Si può dunque auspicare che il governo degli USA predisponga una regolamentazione che vada ad uniformare a livello federale l'impiego della tecnologia di identificazione biometrica, stabilendo dei requisiti specifici per il suo utilizzo nelle attività delle forze dell'ordine, che garantiscono i principi alla base della costituzione.

È proprio a tal fine che molti studiosi ed esperti si stanno appellando alla previsione di una moratoria in vista di una disciplina completa e generale, volta ad evitare la tanto scongiurata sorveglianza di massa.

[304] Matt Cagle, «Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color | ACLU of Northern CA», 11 ottobre 2016, https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

CONCLUSIONE

Giunti al termine delle trattazione emerge con chiarezza come il riconoscimento facciale sia un tema ampiamente controverso, in quanto capace di incidere in modo rilevante sulla privacy di ogni persona: il suo utilizzo costante negli spazi pubblici rischia di indurre le persone a modificare i propri comportamenti (proprio come è accaduto nelle proteste di Hong Kong, dove i manifestanti hanno coperto il loro volto con ombrelli), in quanto non più suscettibili di passare inosservati al resto della collettività. Il rischio che si può correre è il passaggio ad una nuova società, sempre meno libera e più controllata: dallo stato fondato sulla presunzione di innocenza si passa allo stato fondato sulla sorveglianza, che tratta ogni componente della comunità come se stesse per compiere costantemente un illecito e per questo posto sotto l'occhio di una telecamera in modo ininterrotto. È principalmente la capacità di entrare nella vita di ciascuno che rende le TRF peculiari e degne di una regolamentazione *ad hoc* rispetto al resto dell'Artificial Intelligence.

Dall'analisi di tale tecnologia di identificazione biometrica emerge inoltre come questa sia in grado di raccogliere un numero inimmaginabile di dati sensibili, che costituiscono un grande patrimonio per chi li detiene: il pericolo maggiore consta di un loro abuso volto a realizzare molestie e stalking.[305] Tuttavia, una delle questioni principali che permane, anche nel caso in cui esistessero regole chiare che limitano il loro utilizzo, consiste nelle discriminazioni che l'algoritmo del software può produrre nei confronti delle persone nere o di comunità emarginate, dipese dal *training* del programma che viene generalmente realizzato con immagini di uomini bianchi, come dimostrato primariamente dallo studio *Gender Shades* elaborato dalle ricercatrici dell'MIT Media Lab, Joy Boulamwini e Timnit Gebru. Dunque, nel caso in cui ad essere ripresi siano soggetti con la pelle più scura, si verificano errori di *matching* nell'uso della tecnologia, che può condurre ad arresti errati, come si è verificato in numerosi episodi negli Stati Uniti.

L'elaborato si pone l'obbiettivo di analizzare le normative vigenti nei due sistemi giuridici presi in considerazione, al fine di comprendere se sussista una disciplina in grado di garantire il rispetto della privacy e dei diritti fondamentali. Dallo studio

[305] Hartzog e Selinger, «The Inconsentability of Facial Surveillance».

svolto emerge chiaramente l'inadeguatezza dei due ordinamenti confrontati nella regolamentazione della tecnologia di riconoscimento facciale, in quanto impreparati nel disciplinare tutte le implicazioni giuridiche che il suo utilizzo nei luoghi pubblici comporta. Si è verificata infatti l'adozione di tali software presso molte delle forze dell'ordine, in modo particolare negli USA, in assenza però di una reale valutazione a monte sulle capacità dello strumento, equiparandolo quasi ad un normale mezzo da impiegare assieme a quelli già in dotazione presso la polizia. Dunque, per contenere il fenomeno si è reso necessario l'intervento dei giudici volti a supplire, come spesso accade, l'attività del legislatore.

In molti stati e città appartenenti ai due diversi sistemi si sono adottate discipline legislative diverse, volte a limitare o a vietare l'uso di TRF, che contribuiscono alla creazione di uno scenario normativo frammentato ed eterogeneo, incapace di garantire certezza al cittadino, il quale può sentirsi disorientato dalla mancanza di un unico quadro di leggi chiare. L'adozione di moratorie, dirette a sospendere l'impiego delle TRF fintantoché il legislatore non assumerà una posizione in merito al tema, può essere una soluzione temporanea per far fronte alle numerose violazioni che si stanno perpetrando ad opera della polizia, ma non risolve il problema. È necessario che ciascuno dei sistemi normativi presi in esame vada ad analizzare costi e benefici della tecnologia in tema di diritti per comprendere quale sia la migliore normativa che rispetti le libertà delle persone, ma che al tempo stesso riesca a sfruttare i vantaggi che derivano dai processi tecnologici.

Un primo passo in questa direzione è stato effettuato dall'Unione Europea che ha proposto un regolamento dell'AI, stabilendo diritti e obblighi al fine di superare la frammentazione che caratterizza le diverse discipline nazionali, in vista di più ampia armonizzazione delle legislazioni. Tra queste rientra anche il riconoscimento facciale, classificato quale strumento che produce un rischio inaccettabile e pertanto vietato, in quanto capace di generare una sorveglianza di massa. La proposta ammette però suoi impieghi eccezionali laddove risulti fondamentale per la tutela di interessi primari, quali la sicurezza nazionale o la prevenzione di attentati terroristici. Sarà necessario attendere, dunque, una sua approvazione per poter beneficiare di tale regolamentazione.

Negli Stati Uniti manca ancora un progetto uniforme, volto a far sì che tutti i paesi adottino una stessa posizione in merito all'impiego delle TRF: si assiste

piuttosto a posizioni molto diverse negli stati che comportano utilizzi e abusi più frequenti ad opera delle autorità.

Perciò come naturale conclusione dello studio realizzato si può sostenere come l'approccio adottato dalle istituzioni europee potrebbe risultare il più idoneo a garantire da un lato la salvaguardia dei diritti fondamentali delle persone, ma dall'altro a sfruttare, laddove il contesta lo richieda, tale strumento che permette di attingere a potenzialità che la natura umana non è in grado di fornire. È auspicabile, pertanto, che tali due ordinamenti occidentali adottino al più presto regole chiare, onde evitare che tali tecnologie influenzino i comportamenti delle persone al punto tale da mutare il vivere in società e il modo di rapportarsi tra gli individui.

BIBLIOGRAFIA

«A Definition of Artificial Intelligence: Main Capabilities and Scientific Disciplines». Brussels: European Commission, 2019. https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines.

A. Lewis, James, e William Crumpler. «Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape», 29 settembre 2021. https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape.

VSD Lab. «About VSD», s.d. https://vsdesign.org/vsd/.

American Civil Liberties Union. «ACLU-WA Statement on Insufficient Facial Recognition Regulations (SB 6280) Becoming Law», 31 marzo 2020. https://www.aclu.org/press-releases/aclu-wa-statement-insufficient-facial-recognition-regulations-sb-6280-becoming-law.

«ACM Code of Ethics and Professional Conduct», 2018. https://www.acm.org/code-of-ethics.

Agenzia dell'Unione europea per i diritti fondamentali. *Manuale sul diritto europeo in materia di protezione dei dati*. Lussemburgo, 2018. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9113547.

Airoldi, Massimo, e Daniele Gambetta. «Sul mito della neutralità algoritmica». *The Lab's Quarterly*, n. 4 (2018): 25 s. https://www.researchgate.net/publication/332254603_Sul_mito_della_neutralita_algoritmica.

Airports Council International. «Airport Economics Report 2021 - A comprehensive view of the industry's financial performance», 2021.

Amazon staff. «We Are Implementing a One-Year Moratorium on Police Use of Rekognition». Amazon, 10 giugno 2020. https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition.

Amer, Karim, e Jehame Noujaim. *The Great Hack - Privacy violata*, 2019.

An Act To Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials' (2021).

Anonym. «Belgian Police Stop Facial Recognition at Zaventem Airport | Tellerreport.Com», 21 settembre 2019. https://www.tellerreport.com/tech/2019-09-21---belgian-police-stop-facial-recognition-at-zaventem-airport-.BkEeQN8QDH.html.

«Appendix I: Objectives, Scope, and Methodology - Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks». United States Government Accountability Office, giugno 2021.

«Appendix II: Summaries of Selected Federal Agencies' Facial Recognition Technology Activities - GAO-21-526 Facial Recognition Technology». United States Government Accountability Office, agosto 2021.

European Digital Rights (EDRi). «Ban Biometric Mass Surveillance!», 13 maggio 2020. https://edri.org/our-work/blog-ban-biometric-mass-surveillance/.

EPIC - Electronic Privacy Information Center. «Ban Face Surveillance». Consultato 10 febbraio 2022. https://epic.org/campaigns/ban-face-surveillance/.

Ban Facial Recognition. «Ban Facial Recognition». Consultato 7 marzo 2022. https://www.banfacialrecognition.com.

«Ban the scan». Amnesty International. Consultato 5 marzo 2022. https://banthescan.amnesty.org/.

Amnesty International. «Ban the scan - New York City». Consultato 5 marzo 2022. https://banthescan.amnesty.org/nyc/.

Barber, Gregory. «San Francisco Bans Agency Use of Facial Recognition Tech». *Wired*, 14 maggio 2019. https://www.wired.com/story/san-francisco-bans-use-facial-recognition-tech/.

Barrett, Lindsey. «Ban Facial Recognition Technologies for Children—And for Everyone Else». *Boston University Journal of Science and Technology Law* 26, n. 2 (24 luglio 2020). https://ssrn.com/abstract=3660118.

Barrett, Lisa Feldman, Ralph Adolphs, Stacy Marsella, M. Alexei Martinez, e Seth D. Pollak. «Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements». *Psychological Science in the Public Interest* 20, n. 1 (2019). https://journals.sagepub.com/doi/10.1177/1529100619832930.

Bennet, Jared. «Saving face: Facebook wants access without limits». Center for Public Integrity, 2017. https://publicintegrity.org/inequality-poverty-opportunity/saving-face-facebook-wants-access-without-limits/.

Bertuzzi, Luca. «Facial recognition technologies already used in 11 EU countries and counting, report says», 26 ottobre 2021, par. Data protection. https://www.euractiv.com/section/data-protection/news/facial-recognition-technologies-already-used-in-11-eu-countries-and-counting-report-says/.

POLITICO. «Big Brother in Berlin», 13 settembre 2018. https://www.politico.eu/article/berlin-big-brother-state-surveillance-facial-recognition-technology/.

CBS News. «"Big Brother" is big business?», 2013. https://www.cbsnews.com/news/big-brother-is-big-business/.

Big Brother Watch. «Joint statement on police and private company use of facial recognition surveillance in UK», settembre 2019.

Billings, Randy. «Portland councilors approve ban on facial recognition technology». *Press Herald*, 4 agosto 2020. https://www.pressherald.com/2020/08/03/portland-councilors-approve-ban-on-facial-recognition-technology/.

«Biometric face recognition: references for policymaker - An informational document created by the fedid comunity». Federal Identity Community (FedID) Cmmunity, dicembre 2020.

Brown, Julia. «Testimony of Julia Brown, Immigrant Legal Advocacy Project In Support of LD 1585, "An Act To Increase Privacy and Security by Prohibiting the Use of Facial Surveillance by Certain Government Employees and Officials."» Immigrant Legal Advoct Project, 12 maggio 2021. http://www.mainelegislature.org/legis/bills/getTestimonyDoc.asp?id=164320.

Buolamwini, Joy, e Timnit Gebru. «Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification». In *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 77–91. PMLR, 2018. https://proceedings.mlr.press/v81/buolamwini18a.html.

Business, Rachel Metz, CNN. «Beyond San Francisco, more cities are saying no to facial recognition». CNN. Consultato 19 febbraio 2022. https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html.

Bygrave, Lee A. «Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements». *Oslo Law Review* 4, n. 02 (2017): 105–20. https://doi.org/10.18261/issn.2387-3299-2017-02-03.

Cagle, Matt. «Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color | ACLU of Northern CA», 11 ottobre 2016. https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

Carr Smyth, Julie. «States Push Back against Use of Facial Recognition by Police». *AP NEWS*, 5 maggio 2021, par. Ohio. https://apnews.com/article/race-and-ethnicity-health-coronavirus-pandemic-business-technology-e4266250f7e2d691d4d664735c2c6bc0.

Cavoukian, Ann. «Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices», 2009. https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

Centorame, Federica. «Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona». *Rivista italiana di diritto e procedura penale*, n. 2 (2021): 517–23.

Chee, Foo Yun. «EU Privacy Watchdogs Call for Ban on Facial Recognition in Public Spaces». *Reuters*, 21 giugno 2021, par. Technology. https://www.reuters.com/technology/eu-privacy-watchdogs-call-ban-facial-recognition-public-spaces-2021-06-21/.

Chester, Jonah. «Virginia Bill Would Expand Police Use of Facial-Recognition Technology». Public News Service, 17 febbraio 2022. https://www.publicnewsservice.org/index.php?/content/article/77904-1.

Atlas of surveillance. «Chicago Police Department: Face Recognition - Atlas of Surveillance». Consultato 23 febbraio 2022. https://atlasofsurveillance.org/a/aos0978-chicago-police-department-face-recognition.

Clarke, Roger. «Information technology and dataveillance». *Communications of the ACM* 31, n. 5 (1 maggio 1988): 498–512. https://doi.org/10.1145/42411.42413.

«Clearview AI». In *Wikipedia*, 1 gennaio 2021. https://it.wikipedia.org/w/index.php?title=Clearview_AI&oldid=117680562.

«Clearview AI CEO Defends Facial Recognition Software». *Amanpour & Company*, 19 febbraio 2020. https://www.pbs.org/wnet/amanpour-and-company/video/clearview-ai-ceo-defends-facial-recognition-software/.

Clearview AI. «Clearview AI's Revolutionary Facial Recognition Platform Awarded U.S. Patent», 31 gennaio 2022. https://www.clearview.ai/press-release-clearview-ais-revolutionary-facial-recognition-platform-awarded-us-patent.

Cohen, Julie E. «What Is Privacy». *Harvard Law Review* 126, n. 7 (2013): 1904–33. https://www.jstor.org/stable/23415061.

Coluccini, Riccardo. «Lo scontro Viminale-Garante della privacy sul riconoscimento facciale in tempo reale». *IrpiMedia* (blog), 13 gennaio 2021. https://irpimedia.irpi.eu/viminale-garante-privacy-riconoscimento-facciale-in-tempo-reale/.

Coluccini, Riccardo, Laura Carrer, e Philip Di Salvo. «Perché Como è diventata una delle prime città in Italia a usare il riconoscimento facciale». *Wired Italia*, 9 giugno 2020. https://www.wired.it/internet/regole/2020/06/09/riconoscimento-facciale-como/.

Commitee of Ministers. «Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies». Council of Europe, 11 giugno 2013. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c8011.

«Comunicazione della Commissione al Parlamento europeo e al Consiglio. Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia COM(2010)385». Commissione europea, 20 luglio 2010.

«Comunicazione della Commissione Europea al Parlamento europeo e al Consiglio, Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza" dell'aprile 2016», 2016.

Conger, Kate, Richard Fausset, e Serge F. Kovaleski. «San Francisco Bans Facial Recognition Technology». *The New York Times*, 14 maggio 2019, par. U.S. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

Consiglio d'Europa. «Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights». Strasburgo, 14 maggio 2019. https://www.coe.int/en/web/commissioner/view/-/asset_publisher/ugj3i6qSEkhZ/content/unboxing-artificial-intelligence-10-steps-to-protect-human-rights.

Consultative Commitee of the convention 108. «Report on Artificial Intelligence». Council of Europe, 25 gennaio 2019. https://www.researchgate.net/publication/330910567_Consultative_Committee_of_the_Convention_for_the_Protection_of_Individuals_with_Regard_to_Automatic_Processing_of_Personal_Data_Convention_108_Report_on_Artificial_Intelligence_Artificial_Intelligence.

Convention 108. «Guidelines on Facial Recognition Directorate General - Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data», 28 febbraio 2021.

Crawford, Kate, e Trevor Paglen. «Excavating AI: The Politics of Images in Machine Learning Training Sets». Excavating AI, 19 settembre 2019. https://excavating.ai.

Dastin, Jeffrey. «Amazon Extends Moratorium on Police Use of Facial Recognition Software». *Reuters*, 18 maggio 2021, par. Technology. https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/.

De Biase, Luca. «Il difficile equilibrio tra innovazione e tutela dei diritti». *ECONOMIA E POLITICA INTERNAZIONALE*, 22 aprile 2021. https://mydesk24.ilsole24ore.com/crui.

Deckmyn, Dominique, e Nikolas Vanhecke. «De camera ziet u, maar wilt u ook herkend worden?» De Standaard Mobile, 12 ottobre 2019. https://www.standaard.be/cnt/dmf20191011_04658473.

Della Torre, Jacopo. «Novità del Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice». *Diritto penale contemporaneo - Rivista trimestrale*, 2020.

Denham, Elizabeth. «Information Commissioner's Opinion Addresses Privacy Concerns on the Use of Live Facial Recognition Technology in Public Places». ICO, 18 giugno 2021. https://ico.org.uk/about-the-ico/news-and-events/information-commissioner-s-opinion-addresses-privacy-concerns-on-the-use-of-live-facial-recognition-technology-in-public-places/.

European Commission - European Commission. «Discorso sullo stato dell'Unione della Presidente von der Leyen». Text, 15 settembre 2021. https://ec.europa.eu/commission/presscorner/detail/it/SPEECH_21_4701.

U.S. Department of Defense. «DOD Adopts Ethical Principles for Artificial Intelligence», 24 febbraio 2020. https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

Doffman, Zak. «Hong Kong Exposes Both Sides Of China's Relentless Facial Recognition Machine». Forbes, 2019. https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/.

Donovan, Joan, e Chris Gilliard. «Facial Recognition Technology Isn't Good Just Because It's Used to Arrest Neo-Nazis». *Slate*, 12 gennaio 2021. https://slate.com/technology/2021/01/facial-recognition-technology-capitol-siege.html.

Dwoskin, Elizabeth, e Drew Harwell. «Facebook Is Ending Use of Facial Recognition Software, Deleting Data on More than a Billion People». *Washington Post*, 3 novembre 2021. https://www.washingtonpost.com/technology/2021/11/02/facebook-ends-facial-recognition/.

«EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination | European Data Protection Supervisor», 21 giugno 2021. https://edps.europa.eu/node/7131_de.

«EDPS Formal comments on the draft Commission Implementing Decisions». European Data Protection Supervisor, 26 agosto 2020.

University of Arizona News. «Edward Snowden Compares Privacy to Freedom of Speech», 28 marzo 2016. https://news.arizona.edu/story/edward-snowden-compares-privacy-freedom-speech.

Elamroussi, Aya. «This Washington county is the first to ban facial recognition technology, official says». CNN, 2 giugno 2021. https://www.cnn.com/2021/06/02/us/facial-recognition-technology-ban/index.html.

European Commission. «Entry-Exit System», s.d. https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en.

European Commission. «European Criminal Records Information System (ECRIS)», s.d. https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/tools-judicial-cooperation/european-criminal-records-information-system-ecris_en.

European Union Agency for Fundamental Rights. «Under watchful eyes: biometrics, EU IT systems and fundamental rights». Lussemburgo, 2018.

«Explanatory Memorandum COM(2016) 194 final 2016/0106 (COD)». Commissione europea, 6 aprile 2016.

«FACIAL RECOGNITION TECHNOLOGY - Current and Planned Uses by Federal Agencies». United States Government Accountability Office, agosto 2021.

«FACIAL RECOGNITION TECHNOLOGY - Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks». United States Government Accountability Office, giugno 2021.

«Facial recognition technology: fundamental rights considerations in the context of law enforcement». FRA European Union Agency for fundamental Rights, 27 novembre 2019.

«Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses». United States Government Accountability Office, 2020. https://www.gao.gov/products/gao-20-522.

«Facial recognition: the CNIL orders CLEARVIEW AI to stop reusing photographs available on the Internet | CNIL». Consultato 7 febbraio 2022. https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet.

Falce, Valeria. «Intelligenza artificiale, regole a tenuta dei valori UE». *NORME E TRIBUTI*, 6 ottobre 2021, 36. https://mydesk24.ilsole24ore.com/crui.

Ferraris, Valeria. «La profilazione e i suoi rischi». In *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, 69–80. Aracne, 2015.

«Fight for the Future». In *Wikipedia*, 23 gennaio 2022. https://en.wikipedia.org/w/index.php?title=Fight_for_the_Future&oldid=1067408560.

«Frontiere intelligenti». Parlamento europeo, 4 giugno 2015.

Frosini, Tommaso Edoardo. «Il costituzionalismo nella società tecnologica». *Diritto dell'Informazione e dell'Informatica (Il)*, n. 3 (2020): 471–74. blob:https://dejure.it/195053d3-322a-4ec8-8b6b-edda586622e0.

Galbally Herrero, Javier, Pasquale Ferrara, Rudolf Haraksim, Apostolos Psyllo, e Laurent Beslay. «Study on Face Identification Technology for Its Implementation in the

Schengen Information System». Lussemburgo: Publications Office of the European Union, 2019. https://publications.jrc.ec.europa.eu/repository/handle/JRC116530.

Garvie, Clare, Alvaro Bedoya, e Jonathan Frankle. «The Perpetual Line-Up». *Privacy & Technology at Georgetown Law*, 18 ottobre 2016. https://www.perpetuallineup.org/.

Germain, Thomas. «Why Illinois Has Become a Battleground for Facial Recognition Protection». Consumer Reports, 29 maggio 2020. https://www.consumerreports.org/privacy/why-illinois-has-become-a-battleground-for-facial-recognition-protection-a1376302521/.

Greene, Jay. «Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM». *Washington Post*, 11 giugno 2020. https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.

Grother, Patrick, Mei Ngan, e Kayee Hanaoka. «Face Recognition Vendor Test (FRVT) Part 2: Identification». NIST Interagency/Internal Report (NISTIR). National Institute of Standards and Technology, Gaithersburg, 2019. https://doi.org/10.6028/NIST.IR.8271.

Gruppo di lavoro Articolo 29. «Parere 3/2012 sugli sviluppi nelle tecnologie biometriche», 27 aprile 2012. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2375294.

Gruppo di lavoto articolo 29. «Linee guida sul consenso ai sensi del regolamento (UE) 2016/679», 10 aprile 2018. http://ec.europa.eu/justice/data-protection/index_en.htm.

Hardesty, Larry. «Study finds gender and skin-type bias in commercial artificial-intelligence systems». MIT Media Lab, 11 febbraio 2018. https://www.media.mit.edu/articles/study-finds-gender-and-skin-type-bias-in-commercial-artificial-intelligence-systems/.

Hartzog, Woodrow. «BIPA: The Most Important Biometric Privacy Law in the US?» SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 30 ottobre 2020. https://papers.ssrn.com/abstract=3722053.

Hartzog, Woodrow. «Privacy'S Blueprint: The Battle to Control the Design of New Technologies / Woodrow Hartzog». Cambridge (Massachusetts) London (England): Cambridge Massachusetts : London England, 2018.

Hartzog, Woodrow, Neil Richards, e 2020. «Getting the First Amendment Wrong - The Boston Globe». *BostonGlobe.Com*, 4 settembre 2020. https://www.bostonglobe.com/2020/09/04/opinion/getting-first-amendment-wrong/.

Hartzog, Woodrow, e Evan Selinger. «The Inconsentability of Facial Surveillance». *Loyola Law Review* 66 (2019): 101–22. https://law.northeastern.edu/faculty/hartzog/.

Harwell, Drew. «FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches». *Washington Post*, 7 luglio 2019. https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

Haskins, Caroline. «A Second U.S. City Has Banned Facial Recognition». *Vice* (blog), 28 giugno 2019. https://www.vice.com/en/article/paj4ek/somerville-becomes-the-second-us-city-to-ban-facial-recognition.

Haskins, Caroline. «Oakland Becomes Third U.S. City to Ban Facial Recognition». *Vice*, 17 luglio 2019. https://www.vice.com/en/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz.

Hautala, Laura. «San Francisco Becomes First City to Bar Police from Using Facial Recognition». CNET, 14 maggio 2019. https://www.cnet.com/tech/services-and-software/san-francisco-becomes-first-city-to-bar-police-from-using-facial-recognition/.

Henderson, Sarah. «NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software». Text. NIST, 19 dicembre 2019. https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

Hildebrandt, Mireille. «Saved by Design? The Case of Legal Protection by Design». *Nonoethics* 11 (25 agosto 2017): 307–11. https://doi.org/10.1007/s11569-017-0299-0.

Hill, Kashmir. «Facial Recognition Start-Up Mounts a First Amendment Defense». *The New York Times*, 11 agosto 2020, par. Technology. https://www.nytimes.com/2020/08/11/technology/clearview-floyd-abrams.html.

Hill, Kashmir. «The Facial-Recognition App Clearview Sees a Spike in Use after Capitol Attack.» *The New York Times*, 9 gennaio 2021, par. Technology.

https://www.nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html.

Hill, Kashmir. «The Secretive Company That Might End Privacy as We Know It». *The New York Times*, 18 gennaio 2020, par. Technology. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Hill, Kashmir. «What We Learned About Clearview AI and Its Secret 'Co-Founder'». *The New York Times*, 18 marzo 2021, par. Technology. https://www.nytimes.com/2021/03/18/technology/clearview-facial-recognition-ai.html.

Hill, Kashmir. «Wrongfully Accused by an Algorithm». *The New York Times*, 24 giugno 2020, par. Technology. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

Huey, Joanna, Joshua A. Kroll, Solon Barocas, Edward. W. Felten, Joel R. Reidenberg, David G. Robinson, e Harlan Yu. «Accountable Algorithms». *University of Pennsylvania Law Review* 165 (2017): 633 ss. https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/.

Hymas, Charles. «AI used for first time in job interviews in UK to find best applicants». *The Telegraph*, 27 settembre 2019. https://www.telegraph.co.uk/news/2019/09/27/ai-facial-recognition-used-first-time-job-interviews-uk-find/.

BBC News. «IBM Abandons "biased" Facial Recognition Tech», 9 giugno 2020, par. Technology. https://www.bbc.com/news/technology-52978191.

Privacy International. «IBM (Not) Ending Facial Recognition - Our Quick Thoughts», 11 giugno 2020. http://privacyinternational.org/news-analysis/3898/ibm-not-ending-facial-recognition-our-quick-thoughts.

Washington Post. «IBM's Decision to Abandon Facial Recognition Technology Fueled by Years of Debate». Consultato 24 febbraio 2022. https://www.washingtonpost.com/technology/2020/06/11/ibm-facial-recognition/.

«If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine». *Harvard Law Review* 130, n. 7 (2017): 1924–45. http://www.jstor.org/stable/44865635.

Ikeda, Scott. «Maine Becomes First State To Pass Broad Government Ban on Facial Recognition Technology». CPO Magazine, 8 luglio 2021.

https://www.cpomagazine.com/data-privacy/maine-becomes-first-state-to-pass-broad-government-ban-on-facial-recognition-technology/.

American Civil Liberties Union. «Illinois Court Rejects Clearview's Attempt to Halt Lawsuit Against Privacy-Destroying Surveillance». Consultato 23 febbraio 2022. https://www.aclu.org/press-releases/illinois-court-rejects-clearviews-attempt-halt-lawsuit-against-privacy-destroying.

«Interrogazione a risposta immediata in Assemblea 3/02074». CAMERA DEI DEPUTATI, 3 marzo 2021.

Privacy Network. «Italia - Moratoria sul riconoscimento facciale», 2 dicembre 2021. https://www.privacy-network.it/iniziative/italia-moratoria-sul-riconoscimento-facciale/.

Ito, Joy. «AI Engineers Must Open Their Designs to Democratic Control». American Civil Liberties Union, 2 aprile 2018. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/ai-engineers-must-open-their-designs-democratic.

Jauniškis, Pijus. «How Do I Know If the Government Is Watching Me?» Surfshark, 3 novembre 2021. https://surfshark.com/blog/is-the-government-watching-me.

Kaminski, Margot E., e Scott Skinner-Thompson. «Free Speech Isn't a Free Pass for Privacy Violations». *Slate*, 9 marzo 2020. https://slate.com/technology/2020/03/free-speech-privacy-clearview-ai-maine-isps.html.

Kayser-Bril, Nicolas. «At least 11 police forces use face recognition in the EU, AlgorithmWatch reveals». *AlgorithmWatch* (blog), 18 giugno 2020. https://algorithmwatch.org/en/face-recognition-police-europe/.

Kingman, Andy. «In Washington State's landmark facial recognition law, public sector practices come under scrutiny and regulation | Insights | DLA Piper Global Law Firm». DLA Piper, 22 aprile 2020. https://www.dlapiper.com/en/us/insights/publications/2020/04/in-washington-states-landmark-facial-recognition-law-public-sector-practices-come-under-scrutiny/.

Kirkpatrick, Anne E. «Facial Recognition Ordinance Amendment - Supplemental Report». Oakland: Chief of Police, 17 giugno 2019.

Krishna, Arvind. «IBM - Lettera al Congresso», 8 giugno 2020.

Lannan, Katie. «Somerville Bans Government Use Of Facial Recognition Tech», 28 giugno 2019. https://www.wbur.org/news/2019/06/28/somerville-bans-government-use-of-facial-recognition-tech.

Laperruque, Jake. «Testimony in Support of Massachusetts Legislation to Regulate Face Surveillance». Project On Government Oversight, 23 novembre 2021. https://www.pogo.org/testimony/2021/11/testimony-in-support-of-massachusetts-legislation-to-regulate-face-surveillance/.

Lecher, Colin. «Oakland City Council Votes to Ban Government Use of Facial Recognition». The Verge, 17 luglio 2019. https://www.theverge.com/2019/7/17/20697821/oakland-facial-recogntiion-ban-vote-governement-california.

Leslie, David. «Understanding bias in facial recognition technologies: an explainer». *The Alan Turing Institute*, 2020. https://doi.org/10.5281/zenodo.4050457.

Levine, Alessandra S. «Clearview AI on Track to Win U.S. Patent for Facial Recognition Technology». *POLITICO*, 4 dicembre 2021. https://www.politico.com/news/2021/12/04/clearview-ai-facial-recognition-523735.

Lewis, Sarah. «The Racial Bias Built Into Photography». *The New York Times*, 25 aprile 2019, par. Lens. https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html.

Leyen, Ursula von der. «Un'Unione più ambiziosa - Il mio programma per l'Europa», 2019.

«Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia». Commissione europea, 19 febbraio 2020.

Comitato Nazionale per la Bioetica. «L'identificazione del corpo umano: profili bioetici della biometria», 2010. http://bioetica.governo.it/it/pareri/pareri-e-risposte/l-identificazione-del-corpo-umano-profili-bioetici-della-biometria/.

Lisa, Austin. «Privacy and the question of technology». *Law and Philosophy* 22, n. 2 (2003): 119–66. http://www.jstor.org/stable/3505151.

Lynch, Jennifer. «Face Off: Law enforcement use of face recognition technology», febbraio 2018. https://www.eff.org/wp/face-off.

Mac, Ryan, Caroline Haskins, e Logan McDonald. «Clearview AI Says It Will No Longer Provide Facial Recognition To Private Companies». BuzzFeed News, 8 maggio

2021. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies.

Mac, Ryan, Caroline Haskins, e Logan McDonald. «Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA». BuzzFeed News, 27 febbraio 2020. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

Maharrey, Mike. «Now in Effect: Maine Law Limits Government Use of Facial Recognition | Tenth Amendment Center». Tenth Amendment center, 1 ottobre 2021. https://blog.tenthamendmentcenter.com/2021/10/now-in-effect-maine-law-limits-government-use-of-facial-recognition/.

American Civil Liberties Union. «Maine Enacts Strongest Statewide Facial Recognition Regulations in the Country», 30 giugno 2021. https://www.aclu.org/press-releases/maine-enacts-strongest-statewide-facial-recognition-regulations-country.

Max, Gary T., e Valerie Steeves. «From the Beginning: Children as Subjects and Agents of Surveillance». *Surveilance and Society* 7, n. 3/4 (giugno 2010). https://doi.org/10.24908/ss.v7i3/4.4152.

McCarthy, John. «What is Artificial Intelligence?», 12 novembre 2007. http://jmc.stanford.edu/articles/whatisai.html.

McDonald, Caroline Haskins, Ryan Mac, Logan. «Clearview AI Wants To Sell Its Facial Recognition Software To Authoritarian Regimes Around The World». BuzzFeed News, 6 febbraio 2020. https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22.

Merler, Michele, Nalini Ratha, Rogerio Feris, e John R. Smith. «Diversity in Faces». New York: IBM Research, 10 aprile 2019. https://arxiv.org/abs/1901.10436.

Metz, Rachel. «San Francisco just banned facial-recognition technology». CNN, 14 maggio 2019. https://www.cnn.com/2019/05/14/tech/san-francisco-facial-recognition-ban/index.html.

Mobilio, Giuseppe. *Tecnologie di riconoscimento facciale*. Napoli: Editoriale Scientifica s.r.l., 2021.

Morgese, Giuseppe. «La riforma del sistema Dublino: il problema della condivisione delle responsabilità». *Diritto pubblico*, n. 1 (aprile 2020): 103 ss. https://doi.org/:10.1438/96677.

Murphy, Matt. «With Veto Threat, Baker Seeks Several Changes To Landmark Police Reform Bill», diembre 2020. https://www.wbur.org/news/2020/12/10/massachusetts-governor-proposed-amendments-policing-legislation.

«New Facial Recognition Tech "loved" by Law Enforcement: Clearview AI CEO». *Fox Business*, 19 febbraio 2020. http://video.foxbusiness.com/v/6133890195001/.

Niger, Sergio. «Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali / Sergio Niger». <<Le >>monografie di Contratto e impresa. Padova: CEDAM, 2006.

Nissenbaum, Helen. «Protecting Privacy in an Information Age: The Problem of Privacy in Public». *Law and Philosophy* 17, n. 5–6 (1998): 559–96. https://doi.org/10.2307/3505189.

«Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems». European Data Protection Supervisor, 16 aprile 2018.

«Opinion 4/2020 on the European Commission's White Papaer on Artificial Intelligence - A European approach to excellence and trust, cit. p. 27». European Data Protection Supervisor, 29 giugno 2020.

«Opinion 06/2016 on the second EU SmartBorders Package Recommendations on the revised Proposal to establish an Entry/Exit System n. 19». European Data Protection Supervisor, 21 settembre 2016.

«Opinion 7/2017 on the new legal basis of the Schengen Information System». European Data Protection Supervisor, 2 maggio 2017.

Pacino, Giorgia. «Come funziona Sari, il sistema di riconoscimento facciale usato dalla Polizia scientifica». *la Repubblica*, 7 settembre 2018. https://www.repubblica.it/cronaca/2018/09/07/news/come_funziona_sari_il_sistema_di_riconoscimento_facciale_usato_dalla_polizia_scientifica-205804445/.

«Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale)». European Data Protection Supervisor, 18 giugno 2021.

«Parere sul sistema Sari Real Time». GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 25 marzo 2021.

Parlamento Europeo. «Una politica industriale europea globale in materia di robotica e intelligenza artificiale». Gazzetta ufficiale dell'Unione europea, 12 febbraio 2019. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52019IP0081.

Paton-Simpson, Elizabeth. «Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places». *The University of Toronto Law Journal* 50, n. 3 (2000): 305–46. https://doi.org/10.2307/825907.

Patrono, Paolo. «Privacy e vita privata». In *Diritto penale*, XXXV:557–68. De Giuffrè, 1986.

Peaslee, Emma. «Massachusetts Pioneers Rules For Police Use Of Facial Recognition Tech». *NPR*, 7 maggio 2021, par. Technology. https://www.npr.org/2021/05/07/982709480/massachusetts-pioneers-rules-for-police-use-of-facial-recognition-tech.

Perez, Gisela, e Hilary Cook. «Clearview AI: Google, YouTube Venmo and LinkedIn send cease-and-desist letter to facial recognition app that helps law enforcement.» CBS News, 5 febbraio 2020. https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/.

Peyton, McGuireWoods LLP-Janet P. «Virginia's New Consumer Data Protection Act (CDPA)». Lexology, 4 marzo 2021. https://www.lexology.com/library/detail.aspx?g=adaf6e67-d384-4aa5-a50b-ad8e31f43d8c.

Pin, Andrea. «Non esiste la "pallottola d'argento": l'Artificial Face Recognition al vaglio giudiziario per la prima volta». *DPCE online*, 8 gennaio 2020. http://www.dpce.it/dpce-online.html.

la Repubblica. «Polizia di New York, parte dagli USA la campagna per evitare i sistemi di riconoscimento facciale: "Amplificano il razzismo della polizia"», 26 gennaio 2021. https://www.repubblica.it/solidarieta/diritti-umani/2021/01/26/news/profughi-284302004/.

«Privacy Impact Assessment for the ICE Use of Facial Recognition Services DHS/ICE/PIA-054». Homeland Security Investigation, 13 maggio 2020.

«Privacy International | About Privacy International». Consultato 4 febbraio 2022. https://privacyinternational.org/about.

«Provvedimento del 26 febbraio 2020». GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 26 febbraio 2020. https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9309458.

R. Ashman, Charles. «The Assault on Privacy by Arthur R. Miller». *DePaul Review* 20, n. 10 (s.d.). https://via.library.depaul.edu/law-review/vol20/iss4/10.

Ragazzi, Francesco, Ben Wagner, Elif Mendos Kuskonmaz, Ildikó Plájás, e Ruben Van de Ven. «Biometric & Behavioural mass surveillance in EU member states». The Greens/EFA in the European Parliament, ottobre 2021. https://www.greens-efa.eu/biometricsurveillance/.

Ratsimbazafy, Michael. «Maine's Landmark Facial Recognition Law: Preserving Our Rights in the 21st Century». ACLU of Maine, 2 agosto 2021. https://www.aclumaine.org/en/facial-recognition-summer-blog.

Raval, Tony. «Council Post: Examining The San Francisco Facial-Recognition Ban». *Forbes*, 21 giugno 2021. https://www.forbes.com/sites/forbestechcouncil/2019/06/21/examining-the-san-francisco-facial-recognition-ban/.

Ravani, Sarah. «Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns». *San Francisco Chronicle*, 17 luglio 2019, par. Bay Area & State. https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php.

Reclaim Your Face. «Reclaim Your Face: Vietiamo La Sorveglianza Biometrica Di Massa!» Consultato 4 febbraio 2022. https://reclaimyourface.eu/it/.

Rees, Jenny. «Facial recognition: How South Wales Police caught a sexual predator». *BBC News*, 19 febbraio 2021, par. Wales. https://www.bbc.com/news/uk-wales-55842869.

«Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice». European Data Protection Supervisor, 17 novembre 2017.

Reidenberg, Joel R. «Privacy in Public». *University of Miami Law Review* 69, n. 1 (2014). https://repository.law.miami.edu/umlr/vol69/iss1/6.

«Relazione sulla proposta di regolamento UE 2021/0106», 21 aprile 2021.

Remain, H. Jeffrey. «Privacy, Intimacy, and Personhood». *Philosophy & Public Affairs* 6, n. 1 (1976): 44. https://www.jstor.org/stable/2265060.

Horizon 2020 - European Commission. «Responsible Research & Innovation», 2020. https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation.

Richards, Neil, e Woodrow Hartzog. «The Pathologies of Digital Consent». *Washington University Law Review* 96, n. 6 (2019): 1461–1503. https://law.northeastern.edu/faculty/hartzog/.

Garante Privacy. «Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani», 9 marzo 2022. https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9751323.

«Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale ne diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI))». Parlamento europeo, 6 ottobre 2021.

Roth, Lorna. «Looking at Shirley, the Ultimate Norm: Colour Balance, Image Technologies, and Cognitive Equity». *Canadian Journal of Communication* 34 (29 marzo 2009). https://doi.org/10.22230/cjc.2009v34n1a2196.

Ruhrmann, Henriette. «Facing the Future: Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement», maggio 2019.

BBC News. «San Francisco Is First US City to Ban Facial Recognition», 14 maggio 2019, par. Technology. https://www.bbc.com/news/technology-48276660.

Sandler, Rachel. «San Francisco Bans Facial Recognition Technology». *Forbes*, 14 maggio 2019. https://www.forbes.com/sites/rachelsandler/2019/05/14/san-francisco-about-to-ban-facial-recognition/.

Sant, Shannon Van, e Richard Gonzales. «San Francisco Approves Ban On Government's Use Of Facial Recognition Technology», 14 maggio 2019, par. Technology. https://www.npr.org/2019/05/14/723193785/san-francisco-considers-ban-on-governments-use-of-facial-recognition-technology.

Sartor, Giovanni, e Mario Viola De Azevedo Cunha. «Il caso Google e i rapporti regolari USA/EU». *Diritto dell'Informazione e dell'Informatica (Il)*, n. 4–5 (2014): 657–66. https://bibliotecariviste.giuffrefrancislefebvre.it/#/details?id_doc_master=4402550&fromSearch=&fromFilters=true.

Scantamburlo, Teresa, Andrew Charlesworth, e Nello Cristianini. «Machine Decisions and Human Consequences». In *Algorithmic Regulation*, 49–81, 2019. https://doi.org/10.1093/oso/9780198838494.003.0003.

BBC News. «Schools pause facial recognition lunch plans», 25 ottobre 2021, par. Technology. https://www.bbc.com/news/technology-59037346.

Schuba, Tom. «CPD Using Controversial Facial Recognition Program That Scans Billions of Photos from Facebook, Other Sites». Chicago Sun-Times, 29 gennaio 2020. https://chicago.suntimes.com/crime/2020/1/29/21080729/clearview-ai-facial-recognition-chicago-police-cpd.

Shamas, Diala, e Nermeen Arastu. «Mapping Muslims: NYPD Spying and its Impact on American Muslims», marzo 2013. http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

Sharp, Gwen. «Nikon Camera Says Asians: People Are Always Blinking». *TheSociety Pages* (blog), 29 maggio 2019. https://thesocietypages.org/socimages/2009/05/29/nikon-camera-says-asians-are-always-blinking/.

Shwayder, Maya. «Police Facial Recognition Tech Could Misidentify Protesters». Digital Trends, 2 giugno 2020. https://www.digitaltrends.com/news/police-protests-facial-recognition-misidentification/.

Simoncini, Andrea, e Samir Suweis. «Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale». *Rivista di filosofia del diritto, Journal of Legal Philosophy*, gennaio 2019, 87–106. https://www.rivisteweb.it/doi/10.4477/93368.

«Sintesi del parere del Garante europeo della protezione dei dati relativo al primo pacchetto di riforme sul sistema europeo comune di asilo (regolamenti Eurodac, EASO e Dublino) 2017/C 9/04 n.72». Garante europeo della protezione dati, 2017.

«Sistema automatico di ricerca dell'identità di un volto». GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 26 luglio 2018. https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9040256.

«Sistema di videosorveglianza presso lo Stadio Olimpico. Verifica preliminare». GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 28 luglio 2016.

https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/5386852.

Skopek, Jeffrey M. «Reasonable Expectations of Anonymity». *Virgiania Law Review* 101, n. 3 (2015): 691–762. https://www.virginialawreview.org/articles/reasonable-expectations-anonymity/.

Slobogin, Christopher. «Public Privacy: Camera Surveillance of Public Places And The Right to Anonymity». *SSRN Electronic Journal*, 24 febbraio 2003. https://doi.org/10.2139/ssrn.364600.

Solovet, Daniel J. «Conceptualizing Privacy». *California Law Review* 90, n. 4 (2002): 1087–1155. https://doi.org/10.2307/3481326.

Stiano, Alessandro. «Il diritto alla privacy alla prova della sorveglianza di massa e dell'intelligence sharing: la prospettiva della corte europea dei diritti dell'uomo». *Rivista di diritto internazionale*, n. 2 (2020): 511–18. blob:https://dejure.it/5c4aa259-a437-4844-b1e1-442433c71647.

ANSA.it. «Studio Verdi, riconoscimento facciale già in uso in 11 Stati membri - Europa», 29 ottobre 2021. https://www.ansa.it/europa/notizie/sviluppo_sostenibile_digitale/2021/10/29/studio-verdi-riconoscimento-facciale-gia-in-uso-in-11-paesi-ue_d6d3759e-e86c-400a-ab3b-e9aefcfdb5b8.html.

Stumpf, Juliet. «The crimmigration crisis: immigrants, crime, and sovereign power». *American University Lae Review* 56, n. 2 (2016): 367 ss. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=935547.

Surfshark. «Surfshark About Us - products, company, people». Consultato 3 febbraio 2022. https://surfshark.com/it/about-us.

Swan, Betsy. «Facial-Recognition Company That Works With Law Enforcement Says Entire Client List Was Stolen». *The Daily Beast*, 26 febbraio 2020, par. tech. https://www.thedailybeast.com/clearview-ai-facial-recognition-company-that-works-with-law-enforcement-says-entire-client-list-was-stolen.

Surfshark. «The Facial Recognition World Map - Smile You're on Camera», 2019. https://surfshark.com/facial-recognition-map.

American Civil Liberties Union. «The Fight to Stop Face Recognition Technology | News & Commentary». Consultato 7 marzo 2022. https://www.aclu.org/news/topic/stopping-face-recognition-surveillance/.

«The Right to Privacy in the Digital Age». Report of the United Nations High Commissioner for Human Rights. High Commisioner forHuman Rights, 13 settembre 2021.

Tomlinson, Hugh. «Case Law: R (on the Application of Bridges) v Chief Constable of South Wales, Police Use of "automatic Facial Recognition Technology Unlawful – Hugh Tomlinson QC». Inforrm's Blog, 17 agosto 2020. https://inforrm.org/2020/08/17/case-law-r-on-the-application-of-bridges-v-chief-constable-of-south-wales-police-use-of-automatic-facial-recognition-technology-unlawful-hugh-tomlinson-qc/.

Van Noorden, Richard. «The Ethical Questions That Haunt Facial-Recognition Research». *Nature* 587, n. 7834 (18 novembre 2020): 354–58. https://doi.org/10.1038/d41586-020-03187-3.

Vincent, James. «London Police to Deploy Facial Recognition Cameras across the City». The Verge, 24 gennaio 2020. https://www.theverge.com/2020/1/24/21079919/facial-recognition-london-cctv-camera-deployment.

Vincenti, Umberto. *Introduzione all'etica pubblica: Dispense ad uso degli studenti.* Edizioni libreria progetto Padova, 2020.

V.O. Valli, Roberto. «Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini». *il Penalista*, 16 gennaio 2019. https://ilpenalista.it/articoli/focus/sullutilizzabilit-processuale-del-sari-il-confronto-automatizzato-di-volti.

Wagner, Kurt. «Digital Advertising in the US Is Finally Bigger than Print and Television». Vox, 20 febbraio 2019. https://www.vox.com/2019/2/20/18232433/digital-advertising-facebook-google-growth-tv-print-emarketer-2019.

Warren, e Brandeis. «The Right to Privacy». *Harvard Law Review* 4, n. 5 (1890): 193–220. https://doi.org/10.2307/1321160.

Woodruff, Grace. «Maine Now Has the Toughest Facial Recognition Restrictions in the U.S.» *Slate*, 2 luglio 2021. https://slate.com/technology/2021/07/maine-facial-recognition-government-use-law.html.

Writer, Scott. «Lawmakers may limit use of facial recognition software by police in Maine». *Press Herald* (blog), 25 maggio 2021. https://www.pressherald.com/2021/05/25/legislature-may-limit-use-of-facial-recognition-software-by-police-in-maine/.

«XVIII legislatura, Interpellanza urgente 2/01109». CAMERA DEI DEPUTATI, 22 febbraio 2021. https://www.camera.it/leg18/1.

Zalnieriute, Monika. «Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State». *The Columbia Science & Technology Law Review*, 2021.

Ziccardi, Giovanni, e Pierluigi Perri. *Tecnologia e diritto. Informatica e diritto. Data governance, protezione dei dati e gdpr, mercato unico digitale, blockchain, pubblica amministrazione digitale*. Vol. 2. Giuffrè Francis Lefebvre, 2019.

Zoblina, Anastasiia. «Moscow's Use of Facial Recognition Technology Challenged». *Human Rights Watch* (blog), 2020. https://www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged.

Zuddas, Paolo. «Intelligenza artificiale e discriminazioni». Consulta Online - Liber Amicorum per Paquale Costanzo, 16 marzo 2020. https://www.giurcost.org/.

Giurisprudenza

ACLU v. Clearview AI (Corte dell'Illinois 28 maggio 2020).

Big Brother Watch e altri v. UK (Corte europea dei diritti dell'uomo 13 settembre 2018).

Bridges, R (On Application of) v The Chief Constable of South Wales Police EWHC 2341 (admin) (High Court of Justice 4 settembre 2019).

C-203/15 e C-698/15, Tele2 Sverige AB (CGUE 21 dicembre 2016).

C-293/12 e C-594/12 Digital Rights Irleand (CGUE 8 aprile 2014).

California v. Greenwood, 486 U.S. 35 (1988).

Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (Court of Georgia 3 marzo 1975).

Decisione 2008/633/GAI (2008).

Florida v. Riley, 488 U.S. 445 (1989).

Gibson v. Florida Legislative Investigation Committee, 372 U.S. 539 (United States Supreme Court 1963).

Griswold v. Connecticut, 381 U.S. 479 (1965).

Katz v. United States, 389 U.S. 347 (1967).

Kyllo v. United States, 533 U.S. 27 (2001).

Olmstead v. United States, 277 U.S. 438 (1928).

R. (On the Application Of) v. South Wales Police [2020] EWCA Civ 1058 (Court of Appeal 11 agosto 2020).

Rivera v. Google (2017).

Roe v. Wade, 410 U.S. 113 (1973).

S. & Marper v. UK (Corte Europea dei Diritti dell'Uomo 4 dicembre 2008).

Snyder v. Phelps, 562 U.S. 443 (U.S. Supreme Court 2011).

Sommer v. Germany (Corte europea dei diritti dell'uomo 27 aprile 2017).

State of Illinois v. Facebook & Cambridge Analytica (2018).

United States v. Jones, 565 U.S. 400 (2012).

United States v. Miller 425 U.S. 435 (1976) (s.d.).

Legislazione

Art. 3 Trattato sull'Unione Europea (s.d.).

Art. 9 Regolamento UE 2016/679, GDPR (2016).

«Automated Facial Recognition Technology (Moratorium and Review) Bill [HL] - Parliamentary Bills - UK Parliament», 4 febbraio 2020. https://bills.parliament.uk/bills/2610.

Baker D., Charles. Amendments on Police reform bill (2020). https://d279m997dpfwgl.cloudfront.net/wp/2020/12/policing-amendment-letter.pdf.

Carta dei diritti fondamentali dell'Unione Europea (2009).

Chapter 9.64 - REGULATIONS ON CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY | Code of Ordinances | Oakland, CA | Municode Library (2019).

Chief Financial Officers Act (1990).

Circular no. A-130 - Managing Information as a Strategic Resource (2016).

D. lgs. 18 maggio 2018, n. 51, Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. (s.d.).

Decreto 24 maggio 2017, Ministro dell'Interno (s.d.).

Facial Recognition and Biometric Technology Moratorium Act of 2021 (2021

L. 3 dicembre 2021 n. 205, Conversione in legge, con modificazioni, del decreto-legge 8 ottobre 2021, n. 139, recante disposizioni urgenti per l'accesso alle attivitaà culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali.

No Biometric Barries Housing Act (2021).

Ordinance No. 13635 | Code of Ordinances | Oakland, CA | Municode Library (2019).

Primo emendamento delle Costituzione degli Stati Uniti.

Privacy Act - An Act to amend title 5, United States Code, by adding a section 552a, to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes. (1974).

Proposta di regolamento UE 2021/0106, del Parlamento Europeo e del Consiglio del 21 aprile 2021, che stabilisce "regole armonizzate sull'intelligenza artificiale" e modifica alcuni atti legislativi dell'Unione Europea (2021).

Proposta riforma regolamento (UE) 2016/0132 (2016).

Regolamento 2725/2000/CE (2000).

Regolamento (CE) 767/2008 (2008).

Regolamento (UE) 603/2013 (2013).

Regolamento UE 2016/679, GDPR, General Data Protection Regulation (2016).

Regolamento (UE) 2017/2226 (2017).

Regolamento (UE) 2018/1860 (2018.).

Regolamento (UE) 2018/1861 (2018).

Regolamento (UE) 2018/1862 (2018).

Regolamento (UE) 2019/816 (2019).

Regolamento (UE) 2019/817 (2019).

Regolamento (UE) 2019/818 (2019).

La tesi si pone a conclusione della mia carriera universitaria, resa possibile grazie alla presenza di molte persone che nel corso di questi anni mi sono state vicine, supportandomi e credendo in me. Termina così un percorso che mi ha fatto crescere e ha contribuito a formare la persona che ad ora posso dire di essere diventata.

Innanzitutto, vorrei ringraziare il mio relatore, prof. Andrea Pin, per la sua disponibilità e per aver saputo nutrire in me l'interesse per la materia.

Un ringraziamento speciale va ai miei genitori, Giuseppe e Cristina, che mi hanno permesso di arrivare fino a qui, supportandomi giorno per giorno, assecondandomi e incoraggiandomi nel coltivare sempre quel che più mi interessava.

A mia sorella Gessica, che c'è sempre stata, non ha mai smesso di credere in me, anche quando io non lo facevo, mi ha sempre sostenuta e aiutata con la sua gentilezza e premurosità che la contraddistingue, mio punto di riferimento per ogni cosa.

A Tommaso, che ha saputo essere presente in ogni momento, dispensando consigli preziosi e credendo in me, con cui ho condiviso ogni tappa ragguinta.

A Denis, per me fratello maggiore, che ha saputo strapparmi sorrisi anche nei momenti più bui.

Ai miei nonni con cui avrei voluto condividere questo traguardo.

A tutti i miei amici che hanno saputo regalarmi spensieratezza e momenti felici in questi anni.