Università degli Studi di Milano-Bicocca
Dipartimento di Scienze Economico-Aziendali e Diritto per l'Economia

QUADERNI DI DIRITTO DELL'ECONOMIA

La democrazia della società digitale

Tensioni e opportunità

Atti del Convegno 3 dicembre 2021
Università di Milano-Bicocca

a cura di

Elena di Carpegna Brivio e Alessandro Sancino

G. Giappichelli Editore

PREFAZIONE

Francesca Mattassoglio [*]

Il volume curato da Elena Di Carpegna Brivio e Alessandro Sancino giunge sugli scaffali con un tempismo perfetto.

Forse mai, come in questo momento, si sta avvertendo l'urgenza di riflettere sull'impatto della digitalizzazione su un bene delicato e prezioso come la democrazia.

Il processo di innovazione digitale, che può ormai annoverare strumenti come l'intelligenza artificiale, sta rapidamente trasformando la vita di ciascuno di noi, offrendoci, innegabilmente, nuove potenzialità e declinazioni funzionali, che richiedono, però, regole innovative e capaci di fronteggiarne rischi e peculiarità.

Tanto più data l'incredibilità velocità con cui il fenomeno evolve.

In proposito, il pensiero corre immediatamente alla piattaforma ChatGPT, lanciata lo scorso novembre dalla società OpenAI, che si avvale di una intelligenza artificiale di tipo generativo, in grado di creare o generare "nuova" informazione – sia essa un'immagine, un video, contenuti scritti o musicali – partendo dai dati con cui viene alimentata.

Simili risultati, inimmaginabili anche solo fino a poco tempo fa, presentano sviluppi di cui siamo tuttora inconsapevoli e, di conseguenza, accanto alla curiosità, suscitano dubbi e acuiscono i timori che già un'ampia parte di esperti e opinione pubblica riserva al fenomeno.

Anche senza giungere ad abbracciare le posizioni estreme di quanti temono addirittura l'inverarsi di una super intelligenza artificiale, che potrebbe prendere il sopravvento sull'essere umano [1]; numerose ricerche hanno evidenziato

---

* Professore Associato di Diritto dell'Economia, Università degli Studi di Milano-Bicocca.

[1] *Ex multis*, si v. N. BOSTROM, *La superintelligenza. Tendenze, pericoli, strategie*, Torino, 2018.

come spesso le analisi, che poggiano su sistemi di elaborazione automatica, possano essere condotte sulla base di dati errati o, comunque, dare risultati scorretti, oltre che talora discriminatori, per giunta con un ambiguo riparto delle responsabilità.

Proprio per questo, sarà necessario approcciare il fenomeno con estrema cautela e guardare con favore all'affermazione di quel nuovo filone di ricerca incentrato su un uso etico dell'IA [2]. Premesse imprescindibili per addivenire alla costruzione di un contesto regolatorio capace di svilupparne le potenzialità, attenuandone i rischi [3].

Tuttavia, il raggiungimento di un simile obiettivo non sarà semplice.

È infatti già evidente che l'arrivo di questo nuovo modello di intelligenza artificiale generativa rappresenterà un elemento destinato a rendere ancor più complesso il percorso verso l'adozione di un'adeguata cornice normativa e a rallentare, ulteriormente, il processo formativo di quel regolamento europeo sull'intelligenza artificiale, a cui si sta faticosamente lavorando fin dalla primavera del 2021. Senza dimenticare che essa ha addirittura spinto migliaia di nomi noti, tra cui Musk, Wozniak e Harari, a sottoscrivere una lettera aperta[4] che invoca una moratoria di 6 mesi per l'intelligenza artificiale, in attesa che vengano predisposte regole per la sua gestione.

In questo clima di incertezza, non stupisce, pertanto, la scelta, dello scorso 30 marzo, dell'autorità garante della privacy italiana di adottare un provvedimento finalizzato a bloccare l'operatività di ChatGPT per i cittadini italiani, denunciando una serie di violazioni del regolamento n. 679/2018, c.d. GDPR.

Nell'attuale silenzio del regolatore, l'unico baluardo che può essere utilizzato per frenare l'avanzata di una tecnologia così dirompente è, infatti, ancora una volta costituito dalla normativa in materia di tutela dei dati e della privacy.

---

[2] Sui rischi che possono essere causati dall'utilizzo dell'AI, si veda, in particolare, il nuovo filone di ricerca sulla sua etica, tra cui si deve citare L. FLORIDI, J. COWLS, T.C. KING, M. TADDEO, *How to Design AI for Social Good: Seven Essential Factors*, in *Science and Engineering Ethics* 26 (3), 2020, 1771 ss., in *https://doi.org/10.1007/s11948-020-00213-5*; L. FLORIDI, M. TADDEO, *What Is Data Ethics?*, in *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2016,* 374 (2083): 20160360, in *https://doi.org/10.1098/rsta.2016.0360.*

[3] In generale, sul problema della sua regolazione, v. F. PASQUALE, *Le nuove leggi della robotica. Difendere la competenza umana nell'era dell'intelligenza artificiale*, Roma, 2021.

[4] L'intero testo della lettera può essere letto sul sito: *https://www.giurdanella.it/2023/04/sei-mesi-di-moratoria-sugli-esperimenti-di-intelligenza-artificiale-la-lettera-aperta/.*

Non è certo facile esprimere un giudizio in proposito.

Se da una parte, è innegabile che la capacità della piattaforma di raccogliere dati sui suoi interlocutori, che poi vengono utilizzati per l'addestramento degli algoritmi stessi, ponga inevitabilmente delicati problemi di bilanciamento con la disciplina del regolamento privacy; dall'altra non possiamo, tuttavia, ignorare che tale questione è soltanto una delle tante che una simile tecnologia solleva e che dovranno essere risolte per imparare a convivere e a gestire un simile potenziale, al fine di salvaguardare la democrazia di una società destinata inesorabilmente a diventare sempre più digitale.

In tale contesto, il presente volume, che affronta una serie di questioni nodali per la sopravvivenza stessa delle libertà che noi oggi conosciamo, può costituire un utile strumento di riflessione.

INTRODUZIONE
L'UMANITÀ E LA TECNOLOGIA: FINIREMO COME ROBOT?

Alessandro Sancino ∗

L'uso della tecnologia non è neutrale, eppure mai come oggi di fronte a sfide ambientali e sociali che mettono finanche in gioco la sopravvivenza futura del pianeta, le persone umane hanno e avranno sempre più bisogno della tecnologia per governare e domare queste sfide, peraltro create dall'umanità stessa. A tal riguardo, il nostro mondo post-pandemico ha già ampiamente dimostrato che la tecnologia può essere impiegata al servizio della società, ma può essere altresì impiegata per disumanizzare, ad esempio superando l'Homo Sapiens verso forme di Cyborgs [1], oppure sottomettendo un individuo ad un regime di sorveglianza di massa.

La pandemia Covid-19 ha accelerato la trasformazione digitale delle nostre vite e delle nostre istituzioni. Ciò che sembrava impossibile è diventato possibile e si sta ora normalizzando una modalità di lavoro e di organizzare digitale. Il Covid-19 ci ha insegnato quanto sia importante dare informazioni accurate e come, pure in un mondo digitale, le relazioni di prossimità territoriale siano però fondamentali per accedere a servizi di base e per vivere a pieno la propria esistenza.

In un momento storico in cui potrebbe essere in atto perfino un cambiamento antropologico di ciò che è umano e dei suoi confini con la realtà digitale [2], il volume che ho l'onore di introdurre costituisce un approdo, stimolante

---

∗ Alessandro SANCINO è Professore Associato presso l'Università degli studi di Milano Bicocca e Senior Lecturer (fractional appointment) presso The Open University nel Regno Unito. Contatti: alessandro.sancino@unimib.it

[1] CARONIA, A., *Il cyborg. Saggio sull'uomo artificiale*. ShaKe Edizioni, 2008.

[2] HARARI, Y.N., *21 Lessons for the 21st Century:'Truly mind-expanding... Ultra-topical'Guardian*. Random House, 2018.

nei contenuti di frontiera, e sicuro nella solidità degli argomenti proposti, per riflettere sulla relazione tra umano e progresso tecnologico e sulle implicazioni di come questa relazione sta venendo declinata in varie parti del mondo rispetto alla tenuta di una forma ideale di democrazia così come è stata finora concettualizzata dalle Società occidentali.

In ordine di presentazione dei contributi, Mobilio si concentra sulle tecnologie di riconoscimento facciale (TRF) per l'identificazione automatizzata delle persone, mostrando come il loro impiego sia oramai diffuso entro molte delle nostre cosiddette "smart cities". Attraverso un'analisi della disciplina sulla protezione dei dati personali e della proposta a livello di UE per uno "AI Act", Mobilio giunge alla conclusione che «la decisione del legislatore europeo di regolamentare queste tecnologie senza vietarle del tutto sembra essere in astratto legittima, ma le condizioni imposte suggeriscono che forse i tempi non sono ancora maturi per consegnare questo potere di sorveglianza nelle mani delle forze dell'ordine» (Mobilio, 2023 in questo volume).

Nozza muove dall'interrogativo se gli algoritmi hanno pregiudizi e propone un'importante riflessione sulle conseguenze dell'intelligenza artificiale, il cui utilizzo viene sperimentato quotidianamente da molti di noi attraverso l'uso di applicazioni come Siri e Alexa o attraverso la concessione di prestiti. In particolare, il lavoro di Nozza ci aiuta a riflettere rispetto ai bias nell'Intelligenza Artificiale (IA), ossia «l'errore sistematico che si verifica quando un algoritmo fa previsioni o decisioni sistematicamente e costantemente errate per determinati gruppi o individui» (Nozza, 2023 in questo volume). Una delle Sue importanti conclusioni è che l'etica, l'equità e la responsabilità nell'utilizzo dell'IA richiede un approccio olistico alle soluzioni tecniche, rendendosi fondamentale considerare normative e regolamentazioni, il ruolo di ricercatori e sviluppatori di IA, degli utenti finali e di forme di auditing civico affinché i «sistemi di IA siano sviluppati e utilizzati in modo etico e responsabile» (Nozza, 2023 in questo volume). Parallelamente alle innovazioni tecnologiche occorre dunque considerare il loro uso sociale e la governance delle innovazioni tecnologiche sia a livello di regolamentazione di sistema sia a livello di applicazione dell'IA all'interno di istituzioni socio-economiche.

Nel contributo successivo, Rossini fornisce una fondamentale chiarezza sul fenomeno dell'hacking, finora trattato in modo superficiale e, per l'appunto, con un bias tendenzialmente negativo. Bene fa invece Rossini a «mostrare sia lati "positivi" che lati "negativi" della tecnologia informatica e dell'hacking' al fine di 'stimolare una riflessione critica e un pensiero autonomo su questi temi, dai quali poi possa nascere un confronto ricco» (Rossini 2023, in questo volume). Un altro merito della riflessione di Rossini è quello di

fornire esempi concreti su come il positive hacking, definito dall'Autore «come le potenzialità positive che la tecnologia offre ai propri utilizzatori», possa co-produrre valore pubblico con la Pubblica Amministrazione, sfidando quest'ultima a confrontarsi con questo fenomeno e potenzialmente ad istituzionalizzare forme di positive hacking dentro la Pubblica Amministrazione.

Nel settimo capitolo, Sosa Navarro affronta il tema dei Neurorights e parte da alcuni interrogativi che ben rappresentano la portata delle innovazioni tecnologiche a cui siamo difronte: «È possibile immaginare un mondo in cui gli avvocati, invece di fatturare le loro ore, fatturano la loro attenzione, misurata attraverso un elettroencefalogramma (EEG)? È possibile che un imputato riesca a difendersi se le prove a suo carico sono informazioni estratte direttamente dal suo cervello?» (Sosa Navarro 2023, in questo volume). L'Autrice ci aiuta a capire il concetto di Neurorights che sono «dispositivi e procedure utilizzati per accedere, monitorare, indagare, valutare, manipolare e/o emulare la struttura e la funzione dei sistemi neurali delle persone fisiche», focalizzandosi sulle neurotecnologie che «possono (oltre che leggere) alterare l'attività cerebrale, in ragione della loro capacità di sfidare dei beni giuridici che sono alla base del sistema internazionale dei diritti umani» (Sosa Navarro 2023, in questo volume). Come sostenuto dall'Autrice, la partita è importante anche dal punto di vista economico con un mercato globale delle neurotecnologie che dovrebbe crescere a tassi vertiginosi nei prossimi anni, con un valore stimato pari a 21 miliardi entro il 2026. Il Suo contributo, usando le Sue parole, si pone l'obiettivo «di far luce sulle contraddizioni esistenti e sulle disfunzioni dialettiche che influenzano i dibattiti sugli aspetti etici e giuridici delle neurotecnologie ... È necessaria un'azione internazionale urgente per rispondere ai rischi evidenziati» (Sosa Navarro 2023, in questo volume).

Nell'ultimo capitolo del volume, di Carpegna Brivio si concentra sul tema del reputation scoring e deformazioni dello Stato Sociale. Il reputation scoring è «l'assegnazione di un punteggio alla reputazione sociale di una persona» (di Carpegna Brivio, 2023, in questo volume). L'analisi dell'Autrice fornisce numerosi spunti critici, sottolineando come «non tutto, però, nella società umana, si presta ad essere quantificato e rielaborato attraverso la modellazione» e che se applicato allo Stato Sociale «l'uso di tecnologie computazionali e pratiche di reputation scoring rischia di trasformarlo non più in uno strumento per la riduzione delle diseguaglianze sociali, quanto piuttosto un complesso sistema di incentivi e disincentivi che mira a rinforzare diseguaglianze e soggezioni» (di Carpegna Brivio, 2023 in questo volume). Vorrei altresì riportare un passaggio dell'Autrice che sembra stabilire un collegamento importante tra innovazione tecnologica e cittadinanza e ben rappresen-

ta secondo me il pensiero dell'Autrice: «occorre allora riuscire ad affrontare l'innovazione tecnologica come una vera e propria questione di cittadinanza, come definizione di una relazione tra persona e potere che deve essere modellata non soltanto chiedendosi cosa è possibile realizzare ma anche cosa è giusto e desiderabile realizzare» (di Carpegna Brivio, 2023 in questo volume).

Dopo avere brevemente presentato i contributi presenti nel volume, vorrei in chiusura rinnovare il ringraziamento a di Carpegna Brivio per avermi chiamato a scrivere questa introduzione e per essere stata il motore e l'anima di una lezione aperta dell'Università degli studi di Milano-Bicocca che si è sviluppata attraverso gli interventi degli autori di questo volume e il dibattito con gli studenti; è da quella iniziativa che si è originato questo volume.

Infine, se mi è consentita, una riflessione finale. Appare quindi chiaro che gli anni a venire potrebbero significare la fine della liberaldemocrazia rappresentativa oppure il suo radicale rinnovamento. D'altronde, la trasformazione della democrazia appare fortemente interconnessa con l'evoluzione e l'uso di tecnologie come l'IA e il metaverso [3]. A fronte di significative minacce, non possiamo però esimerci dal chiederci come potremmo utilizzare le tecnologie in un modo creativo che sia socialmente e politicamente innovativo [4]. Come richiamato in tutti gli interventi di questo volume, l'uso della tecnologia può essere fatto in modi e con fini molto diversi, dalla promozione di una governance aperta, partecipata e volta alla creazione di valore condiviso e pubblico [5], oppure a fini di monitoraggio e sfruttamento commerciale dei nostri comportamenti come spesso effettuato da molti social networks o siti internet.

Allo stesso modo, come ricordato da di Carpegna Brivio, Paesi come la Cina stanno utilizzando le tecnologie digitali attraverso il sistema di credito sociale (SCS) per stabilire un sistema di punizione/ricompensa che «determina se i cittadini e le organizzazioni sono in grado di accedere a cose come l'istruzione, i mercati e le detrazioni fiscali» [6]. Tuttavia, secondo Lanier e

---

[3] Su questo si vedano ad esempio: BLOOM P. & SANCINO A., *Disruptive Democracy: The Clash between Techno-Populism and Techno-Democrac,* 2019 *y*. SAGE Publications Limited. DE BLASIO E. & SORICE M., *Populism between direct democracy and the technological myth*. Palgrave Communications, 4(1) 2018.

[4] GARCIA-OROSA B., PÉREZ-SEIJO S., *The Use of 360 Video by International Humanitarian Aid Organizations to Spread Social Messages and Increase Engagement*. *VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations*, 31(6), 1311-1329, 2020.

[5] MEIJER A.J., LIPS M. & CHEN K., *Open governance: A new paradigm for understanding urban governance in an information age*. *Frontiers in Sustainable Cities*, 1, 3, 2019.

[6] LIANG F., DAS V., KOSTYUK N. AND HUSSAIN M. M. *'Constructing a data-driven society:*

Weill (2020) ci sono alternative tra la sorveglianza dall'alto della Cina, i giganti della tecnologia occidentale guidati dalla pubblicità negli Stati Uniti, l'Unione europea burocratica e spesso tecnofobica e il caso di Taiwan che combina trasparenza radicale, creatività civica dal basso e innovazioni tecnologiche [7]. Proprio il caso di Taiwan ci consente di citare Audrey Tang, al momento in cui si scrive Ministro per gli Affari Digitali dello Stato di Taiwan, in un passaggio significativo:

> «Quando vediamo "l'internet delle cose", rendiamolo un internet degli esseri. Quando vediamo la "realtà virtuale", rendiamola una realtà condivisa. Quando vediamo "apprendimento automatico", rendiamolo apprendimento collaborativo. Quando vediamo "l'esperienza dell'utente", parliamo dell'esperienza umana. Quando sentiamo "la singolarità è vicina", ricordiamoci: la pluralità è qui» (Tang, 2019) [8].

Se la citazione di Tang potrebbe essere considerata come ancorata ad una spiritualità tecno-ottimista circa il futuro della relazione tra umano e nuove tecnologie, occorre altresì menzionare alcune domande critiche che dovranno animare il dibattito e le scelte in cui tale relazione si estrinsecherà negli anni a venire tramite i molteplici strumenti che la medieranno, dagli Iphones, agli occhiali per il metaverso, alle repository dei Big Data prodotti da noi su Internet, ed in particolare: chi controlla la tecnologia e per quali fini ideologici, politici, economici e materiali? Come potremmo stabilire un controllo democratico sulla produzione di tecnologia per creare potenzialmente un mondo migliore? Come cambia il rapporto con il territorio e cosa significa fare comunità nell'era del digitale?

Non bisogna dimenticare che in una realtà crescentemente virtuale, ci rimane pochissimo spazio per il tipo di interazioni umane spontanee che sono così cruciali per la nostra salute fisica e mentale. Questo libro nasce per discutere queste e altre domande cruciali per il nostro futuro e vuole provare ad

---

China's social credit system as a state surveillance infrastructure', *Policy & Internet*, 10(4), 415-453, citazione riportata da p. 415, 2018.

[7] LANIER J., WEIL E.G. (2020), *How Civic Technology Can Help Stop a Pandemic – Taiwan's Initial Success Is a Model for the Rest of the World*, *Foreign Affairs*, 20th March 2020, available at https://www.foreignaffairs.com/articles/asia/2020-03-20/how-civic-technology-can-help-stoppandemic, accessed on 29th March 2020.

[8] TANG A., *Digital Social Innovation to Empower Democracy. TED x Vitoria Gasteiz*, 2019, 8th May 2019, disponibile qui: https://www.ted.com/talks/audrey_tang_digital_social_innovation_to_empower_democracy, accesso: 07 Maggio 2023.

aprire un dibattito e una consapevolezza pubblica sugli elementi di governance che riguardano una domanda antropologica di fondo: siamo condotti verso un paradigma post-umano in cui umano e digitale si fondono?

L'USO DELLE TECNOLOGIE DI RICONOSCIMENTO FACCIALE DA PARTE DELLE FORZE DELL'ORDINE: BANDIRE O NON BANDIRE?

Giuseppe Mobilio [*]

1. *Introduzione*

Le tecnologie di riconoscimento facciale (TRF) sono una nuova frontiera per l'identificazione automatizzata delle persone e il loro impiego è oramai diffuso entro gli ambienti "smart" delle nostre città [1]. Le *smart cities* sono integrate con telecamere e sensori per raccogliere automaticamente dati tramite lettori di targhe automobilistiche, rilevatori di modelli comportamentali e sistemi di riconoscimento facciale [2]. Le autorità di polizia, in particolare, stanno facendo uso massiccio di questi nuovi canali di informazione e di generazione di dati [3]. La biometria – intesa come riconoscimento automatico di persone sulla base delle loro caratteristiche biologiche o comportamentali [4] – ha confe-

[*] Ricercatore di Diritto costituzionale presso l'Università degli Studi di Firenze.
Contatti: giuseppe.mobilio@unifi.it.

Una prima versione del presente scritto è stata discussa in occasione del convegno "Future-proofing the city: A human rights-based approach to the governance of algorithmic, biometric and smart city technologies", svoltosi il 26 agosto 2022 presso l'Università di Helsinki. Gli atti del convegno sono in corso di pubblicazione sulla Rivista *Internet Policy Review*.

[1] AI NOW INSTITUTE, *AI Now Report 2019*, dicembre 2019.

[2] W. AHMAD, E. DETHY, *Preventing Surveillance Cities: Developing a Set of Fundamental Privacy Provisions*, in *Journal of Science Policy & Governance*, 15(1), 2019, 1 ss.

[3] B. BOWLING, S. IYER, *Automated policing: The case of body-worn video*, in *International Journal of Law in Context*, 15(2), 2019, 140 ss.

[4] C.A. JASSERAND, *Avoiding terminological confusion between the notions of 'biometrics' and 'biometric data': an investigation into the meanings of the terms from a European*

rito alle forze dell'ordine una enorme capacità di identificare gli individui entro spazi pubblici. Le TRF, tuttavia, sono considerate molto più invasive di altre tecnologie biometriche: rispetto alle impronte digitali o ai campioni di DNA, infatti, è molto più facile catturare l'immagine di un volto, dal momento che ciò può avvenire a distanza, con persone in movimento, senza alcun contatto fisico e senza che vi sia alcuna consapevolezza o consenso [5]. I sistemi di riconoscimento facciale sono anche incorporabili in un'ampia varietà di dispositivi, come telecamere a circuito chiuso, *bodycam* o droni, rendendo così il riconoscimento ubiquitario e a basso costo [6]. Non sorprende che, fin dallo scoppiare della pandemia da Covid-19, la sorveglianza biometrica è stata impiegata per il tracciamento dei sintomi e per il monitoraggio del distanziamento sociale [7].

Le TRF, di conseguenza, stanno aumentando esponenzialmente la capacità di sorveglianza della polizia; allo stesso tempo, però, il loro impiego richiede grandi cautele. L'uso di queste tecnologie viene giustificato con il bisogno di perseguire interessi pubblici, come il contrasto del crimine o la ricerca di persone scomparse; tuttavia, esso può risolversi in abusi contro i diritti delle persone o delle minoranze, o persino in forme di sorveglianza di massa da parte di regimi oppressivi [8]. L'interrogativo che sorge, dunque, è se il potere di sorveglianza conferito dalle TRF possa trovare posto all'interno dei sistemi costituzionali. L'obiettivo del presente scritto è di contribuire ad offrire una risposta, attraverso una analisi della legislazione in vigore che si applica alle TRF – nello specifico, la disciplina sulla protezione dei dati personali – e della proposta a livello di UE per uno "AI Act", allo scopo di verificare come esse proteggano i diritti fondamentali in gioco e preservino gli ordinamenti democratici.

La risposta a questo interrogativo non è scontata, se si considera che diversi legislatori e decisori politici hanno bandito le TRF o stabilito una mo-

---

data protection and a scientific perspective, in *International Data Privacy Law*, 6(1), 2016, 68.

[5] Più ampiamente, cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, Napoli, 2021, 11 ss.

[6] I. BERLE, *Face Recognition Technology. Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images*, Springer, Cham, 2020, 2 ss.

[7] M. VAN NATTA *ET AL.*, *The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic*, in *Journal of Law and the Biosciences*, 7(1), 2020, 1 ss.

[8] A.G. FERGUSON, *The Rise of Big Data Policing: Surveillance, Race and the Future of Law Enforcement*, New York University Press, New York, 2017.

ratoria su di esse, come accaduto negli Stati Uniti, dove alcuni Stati o città hanno proibito l'uso di questi sistemi di sorveglianza da parte della polizia [9], o come accaduto in Italia [10]. Alcune voci si sono alzate anche a livello di UE, dove lo *European Data Protection Board* e lo *European Data Protection Supervisor*, nella loro opinione congiunta sulla proposta di *AI Act*, hanno chiesto di valutare l'opportunità di vietare ogni uso dell'IA per il riconoscimento automatico di caratteristiche personali negli spazi pubblici [11]. Questa opzione potrebbe certamente costituire l'*ultima ratio*, ma la vera sfida per la regolazione è di riuscire a bilanciare i rischi e i benefici [12]. Occorre evitare di assolutizzare il concetto di rischio: piuttosto, il rischio dovrebbe essere soppesato in relazione alle circostanze concrete, e quindi bilanciato in quelle che vengono chiamate "optimal precautions" [13]. Dunque, lo sforzo dovrebbe essere quello di cercare di stabilire le condizioni e i limiti per l'uso delle TRF in modo da indirizzarne l'impiego verso valori costituzionali. Solamente quando ciò non sia possibile, allora queste tecnologie andrebbero bandite.

La presente riflessione si concentrerà sull'uso delle TRF da parte della polizia per finalità di pubblica sicurezza, quale scenario in cui i rischi e i benefici collidono più apertamente. Inoltre, verrà preso in considerazione uno degli impieghi di queste tecnologie più pervasivi e discussi, ovvero "in tempo reale" e "dal vivo" entro spazi pubblici, nel quale cioè la sorveglianza è costante, il numero delle persone coinvolte è indeterminato e il riconoscimento avviene istantaneamente. Dopo una breve spiegazione del procedimento di riconoscimento facciale, si descriveranno i possibili usi delle TRF da parte della polizia. In questo modo sarà possibile inquadrare meglio le

---

[9] J. SPIVACK, C. GARVIE, *A Taxonomy of Legislative Approaches to Face Recognition in the United States*, in A. KAK (a cura di), *Regulating Biometrics: Global Approaches and Urgent Questions*, AI Now Institute, settembre 2020, 86 ss.

[10] G. MOBILIO, *I sistemi di identificazione biometrica a distanza: un esempio paradigmatico delle sfide lanciate dalla tecnologia al diritto costituzionale*, in P. COSTANZO, P. MAGARÒ, L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Editoriale Scientifica, Napoli, 2022, 467 ss.

[11] EDPB & EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 giugno 2021.

[12] G.K.Y. CHAN, *Towards a calibrated trust-based approach to the use of facial recognition technology*, in *International Journal of Law and Information Technology*, 29(4), 2021, 307.

[13] A. VERMEULE, *The Constitution of Risk*, Cambridge University Press, New York, 2014.

problematiche emergenti dal punto di vista etico, tecnico, sociale, nonché l'impatto sui diritti fondamentali. Successivamente l'analisi terrà conto di come la normativa – segnatamente la disciplina a livello primario dell'UE e la disciplina a livello secondario sulla protezione dei dati personali – affronta questi rischi tramite il principio di proporzionalità, considerato il principio cardine per stabilire se le TRF debbano essere bandite o meno, ma anche per determinare le condizioni per l'uso da parte delle forze dell'ordine. L'analisi si sposterà quindi sulla proposta di *AI Act* per valutare i progressi e i passi indietro rispetto alla disciplina attualmente in vigore, rimarcando come l'impiego delle TRF potrebbe essere potenzialmente consentito, a patto di stabilire restrizioni particolarmente rigorose.

2. *Uno sguardo all'impiego delle TRF da parte delle forze dell'ordine*

Per secoli i volti delle persone sono stati impiegati dalle forze dell'ordine per identificare le persone e leggerne gli stati d'animo. Oggi vi sono macchine in grado di fare ciò automaticamente grazie ad algoritmi di *machine learning* (ML) e all'intelligenza artificiale (IA)[14]. Per cogliere le implicazioni di questa automazione, tuttavia, occorre chiarire brevemente il funzionamento delle TRF.

Il riconoscimento avviene fondamentalmente grazie ad una procedura articolata in più fasi[15]. *Primo*, dopo che l'immagine di una persona è stata catturata, un algoritmo vi rintraccia il volto al suo interno. *Secondo*, un algoritmo estrae le caratteristiche (c.d. *features*) facciali per creare un modello (c.d. *template*) biometrico, quale rappresentazione numerica che distingue univocamente una persona. *Terzo*, un algoritmo compara il modello così estratto con le immagini facciali raccolte in una galleria (c.d. *watchlist*), in cerca di una corrispondenza. Le persone presenti nella galleria sono state già identificate, così che una corrispondenza consente di collegare il volto della persona nell'immagine con le informazioni appartenenti alla persona nella galleria. La corrispondenza, inoltre, è un processo *probabilistico*, poiché il sistema esprime la somiglianza delle immagini tramite un valore percentuale,

[14] L. URQUHART, B. MIRANDA, *Policing faces: the present and future of intelligent facial surveillance*, in *Information & Communications Technology Law*, 31(2), 2022, 194 ss.

[15] Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., 32 ss.

chiamato "*similarity score*": più alto è questo punteggio, più alta sarà la probabilità che l'immagine campione raccolta corrisponda a quella nella galleria.

Le TRF perseguono fondamentalmente tre scopi principali [16]. Il primo è la *verificazione*, anche chiamata comparazione 1-1, dove il modello estratto dall'immagine è comparato con un unico modello (ad esempio, contenuto in un passaporto) di una persona specifica. Il secondo è l'*identificazione*, anche chiamata comparazione 1-molti, dove il modello estratto è comparato con una galleria di molte immagini (ad esempio, le foto segnaletiche). La terza è la *categorizzazione*, che non mira a identificare una persona, ma piuttosto ad estrarre alcune caratteristiche dall'immagine facciale, come l'età, le origini etniche, il genere, lo stato di salute, sulla base delle quali classificare l'individuo in una o più categorie. Ai fini della presente analisi, ci si concentrerà su identificazione e categorizzazione, cui si farà riferimento tramite il generico "riconoscimento".

Poste queste premesse, è possibile offrire alcuni esempi concreti di utilizzo delle TRF da parte delle forze dell'ordine, distinguendo in base ad alcune variabili, quali lo scopo dell'impiego, le persone sottoposte a riconoscimento, il contesto entro cui avviene il riconoscimento.

Per quanto riguarda lo *scopo* [17], la polizia può usare le TRF per scopi *repressivi*, ovvero per identificare una persona ricercata per un crimine. In aggiunta, le TRF possono essere utilizzate per scopi *investigativi*, ovvero per monitorare i movimenti di una persona in spazi pubblici e, ad esempio, ricostruire le sue interazioni con altre persone dopo la commissione di un crimine. Un esempio significativo di entrambi gli scopi è offerto dalla *South Wales police*, che dal maggio 2017 sta sperimentando un sistema chiamato "*Automated Facial Recognition (AFR) Locate*" per identificare sospettati e altre persone all'attenzione della polizia. Questo sistema – che ha dato origine al famoso caso "Bridges", di cui si dirà più avanti – consente di svolgere una sorveglianza "dal vivo" e "in tempo reale" [18]. Ma le forze di polizia possono fare uso

---

[16] Art. 29WP, *Opinion 02/2012 on facial recognition in online and mobile services*, WP192, 22 marzo 2012.

[17] V.L. RAPOSO, *The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal*, in *European Journal on Criminal Policy and Research*, 2022, 4.

[18] P. FUSSEY, B. DAVIES, M. INNES, *'Assisted' Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing*, in *The British Journal of Criminology*, 61(2), 2021, 325 ss.

delle TRF anche per scopi di *prevenzione*, ovvero per prevenire che un soggetto già identificato possa compiere un altro crimine. In questo caso, non essendosi ancora verificata la violazione della legge penale, si pone un problema di rispetto della presunzione di non colpevolezza. Un esempio riferito a questo scopo è offerto dall'uso delle TRF negli stadi, dove la sorveglianza biometrica è oramai diffusa a partire dal Super Bowl del 2001 di Tampa fino alle Olimpiadi del 2021 di Tokyo, per prevenire dalle risse agli episodi di terrorismo [19].

Per quanto riguarda le *persone sottoposte a riconoscimento*, le TRF possono essere impiegate innanzitutto per ricercare *singole* persone. In Europa, una delle prime e più discusse applicazioni delle TRF è avvenuta durante il carnevale del 2016 a Notting Hill, dove la *Metropolitan Police* di Londra impiegò questi sistemi per ricercare singoli disturbatori [20]. Ma si pensi anche all'uso delle TRF durante la guerra in Ucraina, per identificare i soldati o le vittime del conflitto [21]. Tra gli impieghi più preoccupanti di queste tecnologie vi è tuttavia la capacità di individuare *specifiche categorie* di persone. Un esempio conosciuto è la repressione della minoranza degli Uiguri da parte del governo cinese, perpetrata attraverso tecniche di categorizzazione che consentono di rintracciare i tratti somatici di specifiche regioni facciali in grado di distinguere questa minoranza dal resto della popolazione [22]. Inoltre, le TRF possono essere impiegate per monitorare *tutte le persone* di una società. Il "*Social Credit System*" cinese rappresenta il più sistematico impiego di massa delle TRF [23]. A ciascun cittadino o organizzazione pubblica e privata viene associato un numero di "credito sociale" che, tramite la raccolta automatizzata di informazioni riguardanti la vita pubblica e privata, qualifica il livello di reputazione. Questo impiego apre a scenari molto preoccupanti, non solo in termini di

---

[19] B. HUTCHINS, M. ANDREJEVCIC, *Olympian Surveillance: Sports Stadiums and the Normalization of Biometric Monitoring*, in *International Journal of Communication*, 15, 2021, 363 ss.

[20] BIG BROTHER WATCH, *Face Off. The lawless growth of facial recognition in UK policing*, maggio 2018.

[21] N. MENÉNDEZ GONZÁLEZ. *'Does the end justify the means? Clearview AI and the use of Facial Recognition Technology within the Russia-Ukraine conflict'*, in *The Digital Constitutionalist*, 5 maggio 2022.

[22] W. CUNRUI *ET AL*., *Expression of Concern: Facial feature discovery for ethnicity recognition*, in *WIREs Data Mining Knowl. Discov.*, 9, 2019.

[23] F. LIANG *ET AL*., *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, in *Policy and Internet*, (10)4, 2018, 415 ss.

controllo dell'intera società, ma anche di discriminazioni e violazioni sistematiche dei diritti.

Infine, occorre considerare il *contesto* in cui avviene il riconoscimento. Le TRF possono operare in *ambienti controllati*, ovvero in contesti in cui sono presenti condizioni ottimali (di luce, di posizione delle persone coinvolte, ecc.) e con la consapevolezza e cooperazione delle persone sottoposte a riconoscimento. È il caso, ad esempio, dei controlli *smart* alle frontiere, per i quali si può ricordare il progetto finanziato dall'UE "iBorderCtrl", che mira a perfezionare un sistema di rilevamento automatico dei tentativi di inganno da parte di chi varca le frontiere [24]. Tuttavia, le più comuni applicazioni delle TRF avvengono in *contesti semi-controllati* o *non controllati*, anche chiamati "*in the wild*". Qui le forze dell'ordine impiegano queste tecnologie nelle strade, coinvolgendo un numero indeterminato di persone che possono essere potenzialmente inconsapevoli o ostili a queste forme di sorveglianza. L'accuratezza del riconoscimento può anche essere influenzata da queste condizioni, nella misura in cui i dati raccolti – come si vedrà meglio più avanti – possono non rispettare criteri sufficienti di qualità. Un esempio delle conseguenze che può scatenare l'uso delle TRF in queste circostanze è offerto da quanto accaduto negli USA a seguito dell'uccisione di Breonna Taylor e George Floyd nella primavera del 2020, quando la polizia di molte città ha intensificato l'impiego di queste tecnologie, contribuendo a renderle ancora più invise alla popolazione, specie afroamericana [25].

3. *Specificità e pericoli delle TRF: criticità etiche, tecniche, sociali e giuridiche*

Le TRF hanno avuto una lunga evoluzione fin dalla loro prima apparizione alla Esposizione Universale di Osaka del 1970 o la loro commercializzazione negli USA durante gli anni '90, con una rapida espansione dopo i fatti dell'11 settembre 2001 [26]. Gli esempi più attuali rivelano come le TRF ab-

---

[24] J. SÁNCHEZ-MONEDERO, L. DENCIK, *The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl*, in *Information, Communication & Society*, (25)3, 2022, 413 ss.

[25] N. DAVIES, *US police are using facial recognition technology at protests – adding to systemic racism*, in *Business & Human Rights Resource Center*, 18 agosto 2020.

[26] K.A. GATES, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*, New York University Press, New York – London, 2011.

biano conferito alle forze di polizia un potere di sorveglianza senza precedenti, il quale pone una serie di problemi su diversi ordini.

Sul *piano etico*, queste tecnologie di sorveglianza chiamano in causa molteplici valori riferiti all'essere umano [27], come: autonomia, con riguardo alla consapevolezza e al consenso all'uso delle TRF; non malevolenza, intesa come esigenza di evitare i rischi di riconoscimenti errati; beneficenza, intesa come esigenza di massimizzare i benefici delle TRF nel proteggere la sicurezza; giustizia, intesa come esigenza di non discriminazione ai danni di specifici gruppi; responsabilità, in ordine agli errori e ai danni prodotti da queste tecnologie. Ultimamente, ci sono immediate implicazioni per la dignità umana, la quale richiede che le persone non siano trattate come meri oggetti. Le TRF, invece, producono quella che viene chiamata "informatizzazione del corpo" [28], nella misura in cui le parti del corpo – come il volto – vengono oggettivizzate e divengono fonte di informazioni digitali per controlli esterni automatizzati cui le persone sono sottoposte.

Sul *piano tecnico*, le TRF devono affrontare il problema dell'accuratezza. Queste tecnologie – come detto – operano su base probabilistica e possono dare origine a errori nel caso di falsi-positivi, ovvero quando il software trova una corrispondenza, che invece non c'è, con una immagine nella galleria (dando origine, ad esempio, ad un arresto non giustificato), o falsi-positivi, ovvero quando il software non trova una corrispondenza, che invece c'è, con una immagine nella galleria (consentendo, ad esempio, ad un sospettato terrorista di varcare una frontiera) [29]. Stabilire se una TRF sia più o meno accurata è difficoltoso, poiché vi sono molteplici variabili tecniche di cui tener conto e molti modi per valutare l'accuratezza [30]. Anche i dati, inoltre, influenzano la precisione del riconoscimento. Le TRF sono infatti più inclini a commettere errori quando le immagini catturate sono di scarsa qualità, a causa della loro raccolta in ambienti incontrollati e scenari non cooperativi; o quando le gallerie contengono immagini non omogenee in termini di standard e risoluzione; o quando le gallerie contengono immagini di persone che

[27] G.K.Y. CHAN, *op. cit.*, 323 s.

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

[29] J. BUOLAMWINI *ET AL.*, *Facial Recognition Technologies in the Wild: A Primer*, 29 maggio 2020, 3.

[30] P. FUSSEY, B. DAVIES, M. INNES, *op. cit.*, 337.

si assomigliano fra di loro [31]. Anche la qualità dei dataset utilizzati per allenare gli algoritmi di ML è cruciale, come si dirà più avanti.

Sul *piano sociale*, l'impiego delle TRF divide l'opinione pubblica e non è affatto accettato pacificamente. Nel 2020, l'Agenzia europea per i diritti fondamentali ha reso noti i risultati di una indagine che rivela come solo il 17% delle persone in UE siano disposte a condividere le proprie immagini facciali con le autorità pubbliche per scopi identificativi [32].

Le problematiche menzionate si sommano all'impatto che le TRF producono sui *diritti fondamentali* [33]. Queste tecnologie, infatti, implicano una interferenza con una molteplicità di diritti e libertà [34]. I primi a venire in gioco sono il rispetto della vita privata e la protezione dei dati personali [35]. Il primo può essere considerato come il diritto a godere di una sfera di intimità a livello fisico, psicologico e relazionale [36], la quale è seriamente minacciata da tecnologie così invasive che consentono di monitorare il comportamento e le abitudini delle persone. Il secondo può essere inteso come il diritto a mantenere un controllo sui propri dati, persino in spazi pubblici [37]. Tuttavia, l'uso delle TRF implica la raccolta, comparazione, conservazione e condivisione di immagini facciali e modelli biometrici, riducendo enormemente tale controllo. Altri principi costituzionali con cui queste tecnologie interferiscono sono poi i principi di eguaglianza e non discriminazione [38]. L'uso di queste tecnologie presenta l'alto rischio di generare discriminazioni e diseguaglianze in relazione al sesso, la razza, l'origine etnica, la disabilità, l'età, l'orientamento sessuale, i fattori genetici. Da una parte, è stato già detto come le TRF consentano alla polizia di categorizzare e distinguere le persone in base agli elementi appena menzionati. Dall'altra, come si chiarirà più avanti, le TRF sono suscettibili di essere meno accurate a causa di errori e

---

[31] P. GROTHER, M. NGAN, K. HANAOKA, *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*. NISTIR 8280, dicembre 2019.

[32] T. CHRISTAKIS, *EU citizens reluctant to share their biometric data with public authorities finds FRA*, in *Ai-Regulation.Com*, 3 marzo 2020.

[33] Più ampiamente, cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., 57 ss.

[34] FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, 8 ss.

[35] Artt. 7-8 CDFUE e 8 CEDU.

[36] B.-J. KOOPS *ET AL.*, *A Typology of Privacy*, in *University of Pennsylvania Journal of International Law*, 38, 2017, 483 ss.

[37] S. RODOTÀ, *Tecnologie e diritti*, il Mulino, Bologna, 1995, 108.

[38] Artt. 20-21 CDFUE, 14 CEDU, 3 Cost. it.

bias. La pervasività di queste tecnologie, infine, interferisce con altre libertà e valori costituzionali, direttamente o indirettamente scoraggiandone l'esercizio pure legittimo (c.d. *chilling effect*). È quanto accade con la libertà di riunione e manifestazione del pensiero [39]: l'uso delle TRF in spazi pubblici può scoraggiare le persone dall'esprimere le proprie opinioni, incontrare altre persone o partecipare a manifestazioni pubbliche; tutto ciò con un impatto diretto sul livello di democrazia di un Paese.

Il fatto poi che questo potere di sorveglianza non sia esclusivamente nelle mani di autorità pubbliche origina persino maggiori preoccupazioni. Sono proprio le *imprese private* che sviluppano queste tecnologie e le rendono disponibili alle forze dell'ordine; imprese guidate principalmente da interessi economici e non dall'esigenza di perseguire l'interesse pubblico o proteggere i diritti. Basti pensare al caso di Clearview AI, la famosa start-up che ha sviluppato TRF, vendute a centinaia di agenzie negli USA, grazie al rastrellamento di immagini facciali da internet e da social media senza alcun consenso delle persone o delle piattaforme che le avevano pubblicate [40]. Altri *Big Tech*, come IBM, Microsoft e Amazon, hanno invece deciso di sospendere lo sviluppo e la vendita di TRF alle autorità di polizia negli USA fino a che una legislazione non stabilisca condizioni chiare per evitare potenziali abusi [41].

4. *La giusta misura per l'uso delle TRF nella legislazione vigente*

A questo punto l'interrogativo che sorge è se, e a quali condizioni, le forze di polizia possono usare legittimamente le TRF e in che misura questo impiego può essere limitato dal diritto. Più specificatamente, a livello costituzionale, rispondere a questo interrogativo implica esaminare la legislazione e le condizioni da questa prevista affinché le TRF possano limitare legittimamente i diritti fondamentali. Il cardine per questa analisi è offerto

[39] Art. 11-12 CDFUE, 10-11 CEDU, 17 e 21 Cost. it.

[40] I. NERONI REZENDE, *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective*, in *New Journal of European Criminal Law*, (11)3, 2020, 375 ss.

[41] R. HEILWEIL, *Big Tech Companies Back Away from Selling Facial Recognition Technology to Police. That's Progress*, in *Vox*, 11 giugno 2020.

dall'art. 52.1 della Carta dei diritti fondamentali dell'UE (CFRUE) e, in particolare, il principio di proporzionalità, che offre il criterio per trovare il giusto bilanciamento tra gli obiettivi perseguibili e il sacrificio dei diritti. Ampio riferimento verrà riservato agli indirizzi della Corte di giustizia dell'UE (CGUE) e della Corte europea dei diritti dell'uomo (Corte EDU), che con la propria giurisprudenza, specie sulla protezione dei dati personali, hanno offerto coordinate di lettura imprescindibili.

4.1. *Alla ricerca di una legge per le TRF*

A livello primario, in base all'art. 52.1 della CDFUE, le limitazioni al diritto alla protezione dei dati personali devono innanzitutto "essere previste dalla legge". Il bisogno di una base giuridica è stato interpretato dalla CGUE come l'esigenza che la legge stabilisca "regole chiare e precise" che disciplinino "la portata e l'applicazione" della misura limitativa dei diritti e che impongano "requisiti minimi" in modo che le persone i cui dati sono trattati dispongano di "garanzie sufficienti" per proteggere efficacemente i propri dati contro il rischio di abusi nonché contro eventuali accessi e usi illeciti [42]. Analogamente l'art. 8.2 della CEDU richiede che le limitazioni al diritto al rispetto della vita privata siano "previste dalla legge". Di conseguenza, la Corte EDU ha specificato i requisiti di "accessibilità" e "prevedibilità", chiarendo che la legislazione nazionale deve essere sufficientemente chiara da consentire alle persone di agire consapevolmente in conformità alla legge, da una parte, e deve delimitare chiaramente la portata della discrezionalità delle autorità pubbliche consentendo di prevedere le conseguenze giuridiche, dall'altra [43]. La legge deve quindi stabilire garanzie sufficienti riguardanti la natura, la portata e la durata delle misure limitative dei diritti fondamentali, la loro base giuridica, le autorità competenti ad autorizzare tali misure, a metterle in pratica e a supervisionarle, nonché il tipo di rimedi a disposizione [44].

Al momento, tuttavia, non c'è una legislazione, a livello europeo o na-

---

[42] CJEU, *Digital Rights Ireland and Others*, Joined Cases C-293/12 and C-594/12, 8 aprile 2014, § 54; *Opinion 1/15 of the Court (Grand Chamber) EU-Canada PNR Agreement*, 26 luglio 2017, § 141; *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, Case C-311/18, 16 luglio 2020, § 176.

[43] ECtHR, *Shimovolos v. Russia*, no. 30194/09, 21 giugno 2011, § 68.

[44] *Ibidem.*

zionale, che si rivolga direttamente alle TRF, specialmente per il loro uso a scopi di polizia. Questo, certamente, non vuol dire che non vi sia alcuna regolazione che offra protezione ai diritti e ai valori democratici di fronte a questo potere di sorveglianza. Diviene sempre più importante la disciplina sulla protezione dei dati personali, la quale trova applicazione anche nei confronti delle TRF. Il riferimento, a livello di UE, va alla direttiva (UE) 2016/680, di polizia (o Law Enforcement Directive; LED), che trova applicazione per il trattamento dei dati personali ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, sia che il trattamento avvenga da parte delle autorità pubbliche, sia che esso avvenga da parte di altri enti pubblici o privati incaricati dalla legge di svolgere tali funzioni [45]. Nell'ambito del Consiglio d'Europa, inoltre, occorre tener conto della "Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale", siglata nel 1981 e modificata nel 2018 (Convenzione 108+), che si applica anche al settore pubblico [46]. Recentemente, lo *European Data Protection Board* [47], le autorità nazionali di protezione dei dati e il Comitato consultivo della Convenzione 108+ [48] hanno contribuito a chiarire come questi due atti normativi regolino le TRF. Tuttavia, questa stessa regolazione enfatizza il bisogno di una legislazione che soddisfi i requisiti sostanziali sopra richiamati. La giurisprudenza a livello nazionale e le pronunce delle autorità di protezione dei dati

[45] Così l'art. 3.7 LED. Diversamente, la legislazione applicabile è il regolamento (UE) 2016/679 (General Data Protection Regulation – GDPR), il quale non si applica per il trattamento di dati personali da parte delle "autorità competenti" e per le finalità elencate dalla LED. Nonostante il tentativo di separare i due regimi, il GDPR e la LED non possono essere considerati dicotomici, data l'importanza della legislazione nazionale, ad esempio, nel definire il concetto di "reato", di entità privata incaricata di svolgere tali compiti, le fasi del procedimento penale, o il novero delle attività preventive, potendo quindi condurre all'applicazione dell'una o dell'altro e a una differenziazione tra Stati; cfr. M. BREWCZYŃSKA, *A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation*, in E. KOSTA, R. LEENES, I. KAMARA (a cura di), *Research Handbook on EU Data Protection Law*, Edward Elgar, Cheltenham – Northampton, 2022, 91 SS.

[46] Si veda inoltre la Raccomandazione n. R(87) 15 del Comitato dei Ministri per "regolamentare l'utilizzo dei dati a carattere personale nel settore della polizia", del 17 settembre 1987.

[47] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, 21 maggio 2022.

[48] CONSULTATIVE COMMITTEE OF THE CONVENTION 108, *Guidelines on Facial Recognition*, T-PD(2020)03rev4, 28 gennaio 2021.

personali confermano la necessità di colmare questa lacuna.

Quanto alla prima, bisogna tener conto del famoso caso "Bridges v. The Chief Constable of South Wales Police", in cui la *High Court of Justice of Cardiff*[49] e la *Court of Appeal of London*[50] hanno sottoposto a scrutinio l'uso delle TRF da parte della citata *South Wales police*, per verificare se esso fosse conforme alla LED e alla normativa del Regno Unito, e più in generale hanno offerto elementi per interpretare le regole sopra indicate[51]. Segnatamente, la *Court of Appeal* ha stabilito come la normativa attualmente esistente – per lo più attuativa della LED – non possieda la necessaria "qualità della legge"[52]: di conseguenza tale normativa non risulta sufficientemente specifica per rispondere alla "who question", ovvero all'interrogativo su chi possa essere inserito nelle gallerie, e alla "where question", ovvero in quale luogo il sistema possa essere impiegato; ne consegue che all'operatore di polizia sarebbe rimessa una eccessiva discrezionalità su questi profili. Ad una conclusione simile è giunto il Garante italiano per la privacy nella sua opinione sul sistema "Sari Real Time", ovvero un sistema di riconoscimento facciale "dal vivo" e "in tempo reale" sviluppato per il Ministero dell'interno ma non ancora effettivamente utilizzato[53]. Il Garante ha stabilito come occorra adottare una base legislativa che, «in esito alla ponderazione di tutti i diritti e le libertà coinvolti», renda «adeguatamente prevedibile l'uso di tali sistemi, senza conferire una discrezionalità così ampia che il suo utilizzo dipenda in pratica da coloro che saranno chiamati a disporlo». Il rischio, infatti, è che tali sistemi producano una «evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui».

---

[49] [2019] EWHC 2341 (Admin).

[50] [2020] EWCA Civ 1058.

[51] M. ZALNIERIUTE, *Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State*, in *Columbia Science and Technology Law Review*, 22(2), 2021, 284 ss.; A. PIN, *Non esiste la "pallottola d'argento": l'"artificial face recognition" al vaglio giudiziario per la prima volta*, in *DPCE online*, 4, 2019, 3175 ss.; J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Diritto penale contemporaneo*, 1, 2020, 231 ss.

[52] [2020] EWCA Civ 1058, § 86 ff.

[53] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, 25 marzo 2021.

4.2. *La questione spinosa del rispetto del principio di proporzionalità*

L'art. 52.1 CDFUE, tuttavia, non si limita solamente a stabilire l'esigenza di una legge, ma fa riferimento anche alla necessità che venga rispettato il principio di proporzionalità [54]. Il principio di proporzionalità è considerato uno strumento chiave per il ragionamento giudiziario, che consente alle corti – specie costituzionali e sovranazionali – di vincolare l'intervento dello Stato a diritti e valori costituzionali [55]. Come anticipato, il rispetto di tale principio è una condizione per valutare la legittimità delle misure limitative dei diritti fondamentali. Per svolgere questo tipo di giudizio, la giurisprudenza e la dottrina hanno elaborato un test che ricomprende al suo interno tre sotto-test da svolgere in sequenza [56].

Il primo sotto-test riguarda l'*idoneità* del mezzo impiegato a perseguire gli obiettivi. Il primo interrogativo, dunque, è se l'uso delle TRF da parte della polizia sia adeguato agli obiettivi da essa perseguiti. In questo caso la risposta può generalmente essere considerata affermativa, ma la CGUE richiede una definizione precisa degli obiettivi di polizia, in particolare nel caso di interferenze significative con il diritto alla protezione dei dati personali [57]. Il sotto-test sulla idoneità richiama quindi il bisogno di avere regole più stringenti, come sopra riferito.

Il secondo sotto-test guarda alla *necessità* [58], intesa fondamentalmente co-

---

[54] Oltre alla necessità che le misure limitative dei diritti rispettino il contenuto essenziale di tali diritti e libertà, che apportino limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale definiti dal diritto dell'UE o all'esigenza di proteggere i diritti e le libertà altrui.

[55] T. TRIDIMAS, *The Principle of Proportionality*, in R. SCHUTZE, T. TRIDIMAS (a cura di), *Oxford Principles of European Union Law*, Oxford University Press, Oxford, 2018, 243.

[56] In dottrina, v. G. DE BÚRCA, *The Principle of Proportionality and Its Application in EC Law*, in *Yearbook of European Law 1993*, 13, 1993, 113; A. BARAK, *Proportionality: Constitutional Rights and Their Limitations*, Cambridge University Press, Cambridge, 2012, 243 ss. Sulla giurisprudenza della CGUE, v., da ultimo, L. DALLA CORTE, *On proportionality in the data protection jurisprudence of the CJEU*, in *International Data Privacy Law*, 12(4), 2022, 259 ss.

[57] CGUE, *Tele2 Sverige AB* (C-203/15) *v Post– och telestyrelsen, and Secretary of State for the Home Department* (C 698/15) *v Tom Watson, Peter Brice, Geoffrey Lewis*, Joined Cases C-203/15 and C698/15, 21 dicembre 2016, § 102; Joined Cases C-511/18 and C-512/18, *La Quadrature du Net* (C-511/18 and C-512/18) *v Premier ministre, and Ordre des barreaux francophones et germanophone v Conseil des ministres*, 6 ottobre 2020, § 136.

[58] EDPS, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, 11 aprile 2017.

me "essenzialità" della misura per raggiungere gli obiettivi perseguiti e come esigenza che sia la "minore invasiva" per i diritti in gioco. Quindi, il secondo interrogativo è se sia possibile utilizzare mezzi diversi dalle TRF similmente idonei ma meno invasivi rispetto ai diritti. Sul punto la valutazione deve essere condotta molto attentamente, considerato che ci sono strumenti investigativi che non implicano una sorveglianza automatizzata così pervasiva, non sollevano analoghi problemi etici e non riscontrano simili tassi di errore tecnico.

Il terzo sotto-test guarda alla *proporzionalità in senso stretto*, che implica una più ampia comparazione tra costi, intesi come intensità dell'interferenza con i diritti, e benefici, intesi come importanza degli obiettivi [59]. Di conseguenza, considerando le variabili descritte sopra, quando il test di proporzionalità si riferisce ai costi in termini di impatto delle TRF tiene conto del contesto della sorveglianza (es. spazi pubblici), della portata (es. il numero o l'età delle persone coinvolte), del grado di intrusività (es. identificazione o categorizzazione finalizzata alla profilazione, o la percentuale di errori che possono verificarsi), dei diritti fondamentali coinvolti (compreso il fenomeno del *chilling effect*). Quando invece il test si riferisce ai bisogni e all'importanza delle finalità, tiene conto dello scopo (es. controlli di sicurezza alle frontiere o sorveglianza dell'arredo urbano), o della gravità dei crimini perseguiti (es. terrorismo o reati bagatellari) [60].

5. *L'impiego proporzionato delle TRF secondo la normativa sulla protezione dei dati personali*

Il giudizio sulla proporzionalità delle misure limitative dei diritti è una valutazione che deve essere espressa caso per caso, non solo sul contenuto delle norme, ma anche sui concreti utilizzi di queste tecnologie. Per questo il test di proporzionalità appena ricostruito deve tener conto di come la disciplina sulla protezione dei dati personali affronta il bisogno di un uso proporzionato delle TRF [61]. Allo scopo di stabilire se la normativa sull'uso

---

[59] EDPB, *Guidelines 3/2019 on processing of personal data through video devices*, 20 gennaio 2020.

[60] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, 12 maggio 2022.

[61] L. DALLA CORTE, *op. cit.*, 266; A. GUINCHARD., *Taking Proportionality Seriously: The*

di queste tecnologie da parte della polizia implichi un sacrificio proporzionato dei diritti, occorre quindi guardare a come la disciplina sui dati personali affronta alcuni degli aspetti più delicati in gioco nel test di proporzionalità e che dovranno essere valutati durante l'uso effettivo delle TRF [62]. Le problematiche nel rapporto tra legislazione e proporzionalità che emergeranno saranno prese in considerazione anche al fine di esprimere un giudizio sull'*AI Act*.

La LED segna il passaggio da un approccio rimediale e riparatorio della tutela dei dati personali, volto cioè a offrire protezione una volta che il trattamento illegittimo è avvenuto, ad uno di tipo preventivo e anticipatorio della tutela, volto a porre le condizioni affinché il trattamento illegittimo non debba verificarsi [63]. Si potrebbe dire che l'intera impostazione di questa normativa è strutturata su un approccio basato sul rischio, il quale è a sua volta basato sul principio di proporzionalità [64]. Vi sono molteplici principi e istituti che riflettono questa impostazione. Si pensi al *principio di responsabilità*, secondo cui le forze di polizia, quando usano le TRF, devono mettere in atto «misure tecniche e organizzative adeguate» per garantire, ed essere in grado di dimostrare, il rispetto della normativa sui dati personali [65]. Il rigore di queste misure varia in proporzione alla gravità dei rischi, ovvero la probabilità che i diritti e queste regole possano essere violati [66]. Ma si pensi anche alla *valutazione d'impatto sulla protezione dei dati personali*, che le forze dell'ordine devono svolgere ogni volta che il trattamento dei dati presenti «un rischio elevato per i diritti e le libertà», offrendo una descrizione generale dei trattamenti, una valutazione di tali rischi, le misure previste per affrontarli, le garanzie e le misure di sicurezza per garantire la protezione dei dati

Use of Contextual Integrity for a More Informed and Transparent Analysis in EU Data Protection Law, in *European Law Journal*, 24(6), 2018, 434 ss.

[62] Più in generale, sull'applicazione della normativa sui dati personali alle TRF, cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., 119 ss.

[63] A. MANTELERO, *La gestione del rischio*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, Zanichelli, Bologna, 2019, 473 ss.

[64] R. GELLERT, *Understanding the notion of risk in the General Data Protection Regulation*, in *Computer Law & Security Review*, 34(2), 2018, 279 ss.

[65] Art. 19 LED. N. MENÉNDEZ GONZÁLEZ, *Development or dystopia? An introduction to the accountability challenges of data processing by Facial Recognition Technology*, in *Communications Law*, 26(2), 2021, 87-88.

[66] K. YEUNG, L.A. BYGRAVE, *Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship*, in *Regulation & Governance*, 16, 2022, 146.

personali e per dimostrare la conformità alla normativa [67]. L'attenzione delle riflessioni che seguono verrà però concentrata solo su alcuni profili, per sottolineare il tentativo di imporre un uso proporzionato delle TRF e le relative difficoltà emergenti.

5.1. *I dati biometrici*

La prima barriera contro un uso sproporzionato delle TRF è offerta dal regime giuridico dei dati elaborati. Occorre infatti distinguere tra *dati personali*, come le semplici immagini facciali, e *dati biometrici*, ovvero i dati «ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca» [68]. I modelli biometrici elaborati dagli algoritmi di ML rientrano in questa seconda categoria. Di conseguenza, vige per essi un regime più stringente che consente alle autorità di polizia di trattare tali modelli «solo se strettamente necessario» e «se autorizzato dal diritto» dell'UE o degli Stati [69].

La "*stretta necessità*" richiama il requisito della necessità imposto a livello primario, nelle accezioni di "essenzialità" e "minore invasività" per i diritti in gioco. La LED, tuttavia, stabilisce un requisito molto stringente, imponendo una "assoluta necessità" del trattamento [70]. Tenendo conto dei possibili impieghi delle TRF, per come sopra ricostruiti, le garanzie contro un uso sproporzionato di queste tecnologie devono essere previste su molteplici livelli. Sul piano giuridico, è possibile porre limiti con riferimento agli scopi perseguibili (es. la repressione di reati particolarmente gravi), o agli usi con-

---

[67] Art. 27 LED. Per un tentativo di adeguare la normativa sui dati personali al caso specifico delle TRF, cfr. C. CASTELLUCCIA, D. LE MÉTAYER INRIA *Impact Analysis of Facial Recognition: Towards a Rigorous Methodology*. hal-02480647, 2020.

[68] Artt. 3.13 LED e 6.1 Convenzione 108+. E.J. KINDT, *Having yes, using no? About the new legal regime for biometric data*, in *The Computer Law & Security Review*, 34(3), 2018, 527 ss.

[69] Art. 10.1.a) LE). In alternativa al secondo requisite, i dati biometrici possono essere trattati per «salvaguardare gli interessi vitali» di una persona o se i dati sono «resi manifestamente pubblici dall'interessato». In quest'ultimo caso, però, non è sufficiente rendere pubblica una foto, ad esempio su un social network, ma l'interessato deve aver deliberatamente reso pubblico il modello biometrico.

[70] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, cit., 19.

creti (es. periodo di tempo, area geografica, categorie di persone). A livello tecnico e organizzativo, è possibile imporre misure ulteriori per garantire l'integrità e la sicurezza dei dati (es. tramite la crittografia). A livello procedurale, è possibile stabilire che l'impiego sia autorizzato solamente da un'autorità giurisdizionale.

La "*autorizzazione con legge*", d'altra parte, richiama l'ulteriore requisito stabilito a livello primario della "previsione con legge". Tuttavia, come detto, la mancanza di una normativa specifica sulle TRF significa che non vi è una disciplina per limitare legittimamente i diritti che integri i requisiti sostanziali richiesti. Questa lacuna, inoltre, si risolve nella mancanza di una base giuridica per trattare i dati biometrici ai sensi della LED. In conclusione, vi è bisogno di regole chiare che dettaglino appropriate garanzie sul piano legale, tecnico, organizzativo e procedurale per l'uso delle TRF da parte della polizia.

5.2. *Principi di limitazione delle finalità e minimizzazione dei dati*

Altre previsioni che tentano di indirizzare le forze dell'ordine verso un uso proporzionato delle TRF sono i principi di limitazione delle finalità e minimizzazione dei dati. Il *principio di limitazione delle finalità* impone che i dati siano raccolti per «finalità determinate, esplicite e legittime» e che siano trattati in modo «non incompatibile con tali finalità» [71]. Per questo motivo la normativa sui dati personali definisce anche i confini per il riutilizzo legittimo delle immagini per altri scopi. Anche in questo caso essa richiede l'autorizzazione da parte del diritto UE o degli Stati e che il trattamento sia «necessario e proporzionato a tale altra finalità» [72]. Ne consegue che gli scopi di polizia non possano legittimare di per sé il riuso dei dati, e che le immagini facciali raccolte o i riconoscimenti occorsi durante una indagine non possano essere utilizzati in altre indagini, a meno che «la compatibilità venga esaminata caso per caso e purché la base giuridica includa chiare ed esplicite salvaguardie» [73].

---

[71] Artt. 4.1.b LED e 5.4.b Convenzione 108+.

[72] Art. 4.2 LED.

[73] Art. 29WP, *Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, WP 233, 6. Questo è anche il motive

In base al *principio di minimizzazione dei dati*, invece, i dati trattati devono essere «adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati» [74]. Anche questo principio è rilevante per le TRF, considerato che occorre un enorme numero di immagini sia per allenare gli algoritmi di ML che fanno funzionare queste ultime, sia per costruire le gallerie con cui effettuare la comparazione. Come si dirà a breve, l'uso di immagini fortemente differenziate per allenare gli algoritmi porta a riconoscimenti più accurati. In aggiunta, come specificato dall'autorità garante per la protezione dei dati personali del Regno Unito, le forze dell'ordine possono seguire prassi molto diverse nella creazione delle gallerie, impiegando immagini di persone generalmente all'attenzione della polizia o selezionate in base ai compiti da svolgere (es. eventi sportivi, reati specifici), oppure espandendo indiscriminatamente il numero delle immagini da comparare [75].

Anche questi ultimi due principi, tuttavia, rischiano di mostrarsi inefficaci nella regolazione delle TRF. Come le tecniche di *big data analytics* insegnano, a fianco ad un uso primario delle immagini ve ne sono altri secondari che svelano il "valore opzionale" dei dati, il quale non può essere predefinito [76]. Il riutilizzo dei dati, la creazione dei *dataset* per allenare gli algoritmi e la costruzione delle gallerie sono casi indicativi di come le immagini acquisiscano valore quando trattate per finalità o attività differenti. Dal punto di vista della polizia, questi casi sono sintomatici di una "convenienza pratica" [77] nell'uso dei dati alla quale le forze dell'ordine difficilmente vorranno rinunciare. Per questo occorre una legislazione rigorosa sulle tecnologie che limiti tale tendenza e, incoraggiando un uso proporzionato delle TRF, prevenga così i possibili abusi che possono derivarne.

---

per cui l'art. 6 LED richiede una chiara distinzione tra i dati di differenti categorie di persone, come i sospettati, le vittime o i condannati.

[74] Artt. 4.1.c LED e 5.4.c Convenzione108+.

[75] INFORMATION COMMISSIONER'S OFFICE, *ICO investigation into how the police use facial recognition technology in public places*, 31 ottobre 2019, 14-18.

[76] V. MAYER-SCHÖNBERGER, Y. PADOVA, *Regime Change? Enabling Big Data through Europe's New Data Protection Regulation*, in *The Columbia Science & Technology Law Review*, 17(2), 2016, 317-320.

[77] A. SIMONCINI, E. LONGO, *Fundamental Rights and the Rule of Law in the Algorithmic Society*, in H.-W. MICKLITZ *ET AL.* (a cura di), *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, 2022, 33.

5.3. *Il principio di limitazione della conservazione dei dati*

I due principi appena menzionati operano in continuità con il *principio di limitazione della conservazione*, secondo cui i dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore al conseguimento delle finalità per le quali sono trattati [78]. Secondo quanto stabilito dalla CGUE, la conservazione dei dati deve «rispondere sempre a criteri oggettivi, istituendo un rapporto tra i dati da conservare e l'obiettivo perseguito» [79]: quando questa connessione è interrotta e non esiste più una base giuridica per il trattamento, i dati devono essere cancellati o resi anonimi. Pertanto, per quanto riguarda le attività di polizia, il periodo di conservazione dovrebbe variare, ad esempio, in funzione della conclusione di una specifica indagine o dell'emanazione di una sentenza definitiva. Nel caso delle TRF, bisogna anche considerare gli esiti del riconoscimento: se non c'è corrispondenza, le immagini del volto e i modelli biometrici non possono essere conservati e devono essere automaticamente cancellati; se c'è corrispondenza, questi dati (e i rapporti di corrispondenza) possono essere conservati per un tempo strettamente limitato, previsto dalla legge con le necessarie garanzie [80].

Dunque, la legislazione nazionale può prevedere un sistema misto che combina limiti di tempo massimi con un riesame periodico della necessità di custodire i dati per un ulteriore periodo, da valutare in termini di necessità e proporzionalità [81]. A questo proposito, è improbabile che la conservazione dei dati per scopi di intelligence o di prevenzione superi un rigoroso test di proporzionalità, poiché in questi casi le immagini vengono custodite, soprattutto nelle gallerie, senza alcun reato specifico da perseguire e quindi senza alcun termine. Il principio di limitazione della conservazione è quindi un esempio paradigmatico di come le norme giuridiche debbano sostenere il test di proporzionalità ponendo un limite finale al trattamento dei dati e all'uso delle TRF, il quale può essere superato solo sulla base di una valutazione rigorosa.

---

[78] Artt. 4.1.e LED e 5.1.e Convenzione 108+.

[79] CGUE, C-203/15 e C-698/15, *Tele2 Sverige AB*, cit., § 110.

[80] Consultative Committee of the Convention 108, *Guidelines on Facial Recognition*, cit., 12.

[81] Art. 29WP, *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)*, WP 258, 29 novembre 2017, 4.

5.4. *Il diritto di ricevere informazioni e gli altri diritti conseguenti*

Il principio di proporzionalità viene in gioco anche con altri diritti fondamentali sanciti dalla normativa sulla protezione dei dati, ovvero il diritto di ricevere alcune *informazioni* circa l'impiego delle TRF, come l'autorità procedente, le finalità del riconoscimento e l'esistenza di altri diritti [82]. Questo diritto ad essere informato è infatti la precondizione per l'esercizio di *ulteriori diritti*, come quello di accesso ai dati raccolti, alla rettifica e alla cancellazione, specialmente in caso di inaccuratezza dei dati (es. scarsa qualità delle immagini) o impiego illegittimo [83]. L'importanza di questi diritti è stata sottolineata dal Commissario per la protezione dei dati di Amburgo, che nel 2019 ha ordinato alla polizia di cancellare il *database* che conteneva materiali di videosorveglianza raccolti per perseguire, tramite TRF, coloro che durante le proteste al Summit G20 del 2017 incorsero in reati [84]. Il Commissario ha censurato, tra l'altro, il fatto che le persone coinvolte non fossero consapevoli della raccolta delle immagini e quindi non fossero in condizione di esercitare i propri diritti [85].

Ad ogni modo, questi diritti incontrano delle limitazioni in proporzione al bisogno di proteggere altri interessi pubblici. La legislazione nazionale, infatti, può porre limiti per non pregiudicare le indagini, la prevenzione o il perseguimento di reati, o la tutela della sicurezza pubblica [86]. Tuttavia, nel rinviare a tale legislazione, la normativa europea concede troppa discrezionalità agli Stati. La LED non specifica alcun requisito minimo per le legislazioni nazionali, a parte un implicito riferimento al principio di proporzionalità. Pertanto, ogni Stato può bilanciare autonomamente gli interessi in gioco,

---

[82] Artt. 13 LED e 8 Convenzione 108+. A differenza del GDPR, la LED non enuncia esplicitamente il principio di trasparenza. Altre informazioni, come la base giuridica del trattamento o il periodo di conservazione, devono essere fornite agli interessati in "casi specifici" (art. 13.2 LED), riferiti a situazioni in cui gli interessati devono essere messi a conoscenza del trattamento per esercitare efficacemente i loro diritti; cfr. EDPB, *Guidelines 05/2022*, cit., 22.

[83] Artt. 14 e 16 LED.

[84] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Anordnung "Einsatz der Gesichtserkennungssoftware „Videmo 360" durch die Polizei Hamburg zur Aufklärung von Straftaten im Zusammenhang mit dem in Hamburg stattgefundenen G20-Gipfel", 18 dicembre 2018.

[85] T. Raab, *Germany. Video Surveillance and Face Recognition: Current Developments*, in *European Data Protection Law Review,* 5(4), 2019, 544 ss.

[86] Artt. 13.3, 15 e 18 LED, e 9.2 Convenzione 108+.

definire gli scopi o i reati che possono giustificare tali limitazioni e le informazioni che possono essere negate, e quindi definire il livello di consapevolezza della popolazione sottoposta alle TRF. Eppure, è proprio l'uso non trasparente di queste tecnologie da parte della polizia, unitamente alla percezione di essere esposti a forme di sorveglianza così controverse, che contribuiscono a spiegare le preoccupazioni e le proteste scoppiate negli Stati Uniti per l'uso delle TRF nei confronti della popolazione afroamericana [87]. Il caso dei diritti in questione, quindi, è esemplificativo della necessità di avere una legislazione dettagliata, che però non svuoti le garanzie fornite ai cittadini sottoposti a TRF.

5.5. *I* bias *e le discriminazioni*

Infine, c'è un aspetto da considerare nella valutazione della proporzionalità, anch'esso legato alle proteste appena citate, e che è forse la maggiore fonte di preoccupazione per l'uso delle TRF. È il caso dei *bias*, o distorsioni, che possono portare a errori e imprecisioni nel riconoscimento e, di conseguenza, a discriminazioni razziali, etniche e di genere. Questi rischi devono essere valutati come un costo dell'utilizzo delle TRF durante il test di proporzionalità. Molte forme di *bias* possono affliggere questi sistemi [88], ma qui è sufficiente concentrarsi su quelli che si verificano all'interno dei *dataset* utilizzati per addestrare gli algoritmi di ML. A questo proposito, i *bias* possono verificarsi quando gli algoritmi vengono allenati su dati distorti o apprendono da un campione distorto [89]. L'accuratezza degli algoritmi che eseguono automaticamente l'identificazione sarà quindi compromessa se i dati di addestramento riflettono *bias* impliciti [90]. Pertanto, maggiore è il "pluralismo" e la varietà dei dati utilizzati in relazione al sesso, all'età e all'origine

[87] D. WILLIAMS, *Fitting the Description: Historical and Sociotechnical Elements of Facial Recognition and Anti-Black Surveillance*, in *Journal of Responsible Innovation*, 7(1), 2020, 74 ss.

[88] M. VEALE, R. BINNS, *Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data*, in *Big Data & Society*, 4, 2017, 1 ss.; S. BAROCAS, A.D. SELBST, *Big Data's Disparate Impact, in California Law Review*, 104(3), 2016, 671 ss.

[89] F.Z. BORGESIUS, *Discrimination, artificial intelligence, and algorithmic decision-making. Study for the Council of Europe*, 2018, 17.

[90] D. LESLIE, *Understanding bias in facial recognition technologies: an explainer*, The Alan Turing Institute, 2020.

etnica, maggiore è la capacità del sistema di identificare le persone. Studi recenti, tuttavia, dimostrano che le persone con la pelle scura e le donne sono fortemente sottorappresentate in questi *dataset* [91]. Pertanto, le donne con la pelle scura sono associate a tassi di errore di riconoscimento facciale più elevati rispetto agli uomini con la pelle chiara di origine caucasica, soprattutto nel caso di ambienti non controllati [92].

Altre persone che possono subire discriminazioni a causa della minore accuratezza delle TRF sono i minori, gli anziani e le persone con disabilità. In relazione all'*età*, occorre prestare la dovuta attenzione all'alterazione temporale degli elementi fisici utilizzati per il riconoscimento [93]. Per quanto riguarda le *disabilità*, inoltre, è necessario considerare le conseguenze derivanti da incidenti o sindromi specifiche che possono alterare lo stato morfologico e comportamentale di una persona [94].

La normativa sulla protezione dei dati personali affronta il problema dei *bias* affermando che i dati, anche quando vengono utilizzati per allenare le TRF, devono essere «esatti e, se necessario, aggiornati» [95]. Per questo motivo, le forze di polizia che desiderano utilizzare queste tecnologie devono essere in grado di dimostrare l'assenza di *bias*. Come mostra anche il caso "Bridges", le autorità pubbliche devono valutare la composizione demografica di ciascun *dataset* usato per l'addestramento degli algoritmi, direttamente o attraverso una verifica indipendente, per determinare che non presenti *bias* ai danni di un particolare gruppo demografico. Nessuna ragione di riservatezza commerciale avanzata dal produttore del sistema può giustificare l'omissione di questa valutazione [96]. Contrariamente, questi strumenti di *smart policing* sarebbero legalmente ed eticamente inaccettabili.

Tuttavia, l'obiettivo di eliminare i *bias* non è facilmente raggiungibile. Dal punto di vista giuridico, la verifica della presenza di queste distorsioni non è una giustificazione autonoma per il trattamento di dati biometrici. Per-

---

[91] M. MERLER *ET AL.*, *Diversity in faces*, arXiv:1901.10436v6, 8 aprile 2019.

[92] J. BUOLAMWINI, T. GEBRU, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 81, 2018, 77 ss.; P. GROTHER, M. NGAN, K. HANAOKA, *op. cit.*

[93] FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, cit., 90.

[94] S. BYRNE-HABER, *Disability and AI-Bias*, *Medium*, 11 luglio 2019.

[95] Art. 4.1.d LED.

[96] EWCA Civ 1058, § 199.

tanto, potrebbe non essere attualmente chiaro in che misura il trattamento per tale finalità sia considerabile di per sé legittimo [97]. Inoltre, è molto difficile dimostrare che una persona abbia subìto una discriminazione proprio a causa della scarsa qualità del *dataset* di allenamento degli algoritmi. Infine, l'uso diffuso di TRF addestrate su dati non rappresentativi rende difficile sostituire o correggere i sistemi attualmente in uso [98]. È chiaro, quindi, che la legislazione che regolamenta le TRF deve essere molto cauta nel valutare i potenziali benefici rispetto ai possibili, gravi svantaggi.

6. *Il futuro della regolazione delle TRF: l'*AI Act

Il tentativo di adottare una normativa che stabilisca condizioni più severe per un uso proporzionato delle TRF è offerto dalla proposta di regolamento "che stabilisce norme armonizzate sull'intelligenza artificiale" (c.d. *AI Act*), ancora in fase di approvazione al momento della stesura di questo contributo [99]. Le istituzioni dell'UE hanno preparato il terreno con diversi documenti, come gli "Orientamenti etici per un'IA affidabile", prodotte dal Gruppo di esperti ad alto livello sull'IA nel 2019, o il "Libro bianco" sull'IA pubblicato nel 2021 dalla Commissione europea, che hanno posto le basi per un approccio "umano-centrico" [100]. L'obiettivo è, da un lato, implementare un'IA affidabile e, dall'altro, facilitare lo sviluppo di un mercato unico digitale nell'UE.

L'*AI Act* impiega un approccio basato sul rischio [101], distinguendo tra usi dell'IA che creano "rischi inaccettabili", "rischi elevati" e "rischi bassi" o "minimi", ciascuno associato a diverse condizioni. All'interno della prima categoria, la proposta vieta «l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di

---

[97] FRA, *Bias in Algorithms – Artificial Intelligence and Discrimination*, 2022, 26.

[98] P. HACKER, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law*, in *Common Market Law Review*, 55(4), 2018, 1150.

[99] Il riferimento nel testo è al *General Approach* del Consiglio (25 novembre 2022) [https://artificialintelligenceact.eu/documents/].

[100] L. FLORIDI, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in *Philosophy & Technology*, 34, 2021, 215 ss.

[101] G. DE GREGORIO, P. DUNN, *The European risk-based approaches: Connecting constitutional dots in the digital age, in Common Market Law Review*, 59(2), 2022, 473.

contrasto» [102]. Il divieto si applica proprio alle TRF discusse finora, considerate «particolarmente intrusive» [103]. Tuttavia, la proposta prevede eccezioni così ampie a questa regola generale che difficilmente sembra si possa parlare di un vero e proprio divieto [104].

In primo luogo, le forze di polizia possono impiegare le TRF quando «strettamente necessario» per gli *obiettivi* di: ricerca delle vittime di reati; prevenzione di una «minaccia specifica, sostanziale e imminente» alla vita delle persone o a un'infrastruttura critica, o un attacco terroristico; perseguimento degli autori o dei sospettati di reati puniti con una determinata pena ai sensi della Decisione sul mandato d'arresto europeo [105], o della legislazione degli Stati membri. L'*impiego effettivo* delle TRF, quindi, deve tenere conto di diversi elementi: la natura della situazione che dà origine al possibile utilizzo, e le conseguenze per i diritti e le libertà. La polizia deve rispettare «le tutele e le condizioni necessarie e proporzionate», per quanto riguarda «le limitazioni temporali, geografiche e personali» [106]. Inoltre, ogni singolo utilizzo *deve essere autorizzato* da un'autorità giudiziaria nazionale o da un'autorità amministrativa indipendente (ad eccezione dei casi urgenti, per i quali la convalida deve comunque essere richiesta «senza indebito ritardo durante l'utilizzo del sistema di IA»), sulla base di «prove oggettive» e di «indicazioni chiare» in termini di necessità e proporzionalità rispetto agli obiettivi [107]. Gli *Stati membri* dovranno specificare le regole per tale autorizzazione e potranno anche prevedere la possibilità di limitare l'impiego delle TRF in relazione ai reati da perseguire [108]. Le norme nazionali saranno indispensabili, poiché il futuro *AI Act* non potrà essere invocato come base giuridica sufficiente ai sensi delle disposizioni della LED [109]. Da ultimo, le TRF sono anche espressamente soggette alle condizioni stabilite per la seconda categoria degli usi "*ad alto rischio*" dell'IA [110]. Il nuovo regime si ispira a

---

[102] Art. 5.1.d *AI Act*.

[103] Cons. 18 *AI Act*.

[104] N.A. SMUHA *ET AL*., *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, 5 agosto 2021, 25.

[105] Council Framework Decision 2002/584/JHA (13 giugno 2002).

[106] Art. 5.2 *AI Act*.

[107] Art. 5.3 *AI Act*.

[108] Art. 5.4 *AI Act*.

[109] Cons. 23 *AI Act*.

[110] Allegato III.1 *AI Act.*